AU/AF FELLOWS/NNN/2004-00

AIR FORCE FELLOWS (SDE)

AIR UNIVERSITY

EMPOWERING FIRST RESPONDERS –

PEER-TO-PEER TECHNOLOGY

by

Mark D. Bontrager, Lt Col, USAF
Randall J. Richert, Lt Col, USAF

A Research Report Submitted to Air Force Fellows, CADRE/AR

In Partial Fulfillment of the Graduation Requirements

Advisors: Professor Clifford Singer
Director, Program in Arms Control, Disarmament, and International Security, University of Illinois

Dr. Charles Pentland
Director, Centre for International Relations, Queen's University

____
CADRE/AR

Maxwell Air Force Base, Alabama

April 2004

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Empowering First Responders - Peer-to-Peer Technology	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University School of Advanced Air and Space Studies Maxwell AFB, AL 36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**111**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

Contents

Page

Illustrations

Page

Acknowledgments

The authors would like to acknowledge several people for their assistance during the research for this paper.

Lt Col Mark Bontrager would like to thank Professor Clifford Singer and the staff of the Program in Arms Control, Disarmament and International Security (ACDIS) for their outstanding support throughout the year of study at the University of Illinois. Dr. Matthew Rosenstein, Ms. Sheila Roberts, Ms. Becky Osgood and Ms. Jessica Moyer all provided tremendous moral and administrative support throughout the year.

I would have never attempted to tackle this subject without the “nudging” of Mr. Earl Wardell of Decisive Analytics. He got me started on investigating the possibilities of Peer-to-Peer Technology for the warfighter in 2001 and encouraged me to take the next step and apply it to the new frontline warriors – the first responders.

I especially want to thank Major General Dale Myerrose, USNORTHCOM Director of Architectures and Integration for his valuable time at the start of this project. Of special note are the various people who spent their valuable time educating me on the challenges of their domains; specifically, Col Michael Curtis, Lt Col Tom Hains, CDR Joel Swanson and Mitch Daigrepont from USNORTHCOM/J6; John Anderson, Former El Paso County Sheriff; Richard Jaehne and Nancy Mason from the Illinois Fire Services Institute; and Fred Davis and Bill Henry of the Capital Wireless Integrated Network.

Finally, my three boys Joshua, Daniel and Timothy deserve special note for their selfless understanding when Daddy was always disappearing to the office to "study." I am forever indebted to my lovely wife, Julie who supports me daily with encouragement and strength—my gratitude goes beyond words.

Lt Col Richert would like to thank the members and staff of the Queen's University Centre for International Relations, Kingston, Ontario. Especially the Director, Dr. Charles Pentland, Dr. Kim Nossal (Acting Director), Ann Libick and Maureen Halsall (administrative assistants), Dr. Dave Haglund, Brig Gen (ret.) Don Macnamara (CAF), Brig Gen (ret.) William Richard (CAF), Col (ret.) Glenn Brown (RCN & CAF), Lt Col Terry Loveridge (PPCLI), Lt Col Uli Shultz (Luftwaffe), Lt Col John Blaxland (Royal Australian Army), and Lt Col Casey Haskins (USA). Additional thanks go out to Professors Sean Maloney and Kerim Ouesman (Royal Military College of Canada), Mr. Joel Leason from the International Association of Chiefs of Police, and, Inspector Merle Foster and Sergeant Roy Kendall of the Belleville, Ontario Police Department. A special thanks goes out to General Shamess, USAF Director of Security Forces, for allowing me this time away and for his ideas on improving interoperability. And to the coaches, staff, players and fans of the Queen's University Football team-Cha Gheill! Finally, I would especially like to thank my family for all their support during our year in the "Great White North."

Finally, both authors want to express sincere appreciation to staff of the Air Force Fellows office at the Center for Advanced Research and Education at Maxwell AFB for both financial and administrative support for this research effort. Special thanks go to Ms. Dee Taylor and Ms. Betty Littlejohn for their responsive and professional support

throughout the year. Additionally, we thank the USAF Security Forces Battlelab for their support both academically and financially.

Abstract

The terrorist attacks of September 11th, 2001, marked a watershed event for America. No longer can it be expected that the American military will fight our nations battles on foreign lands while America's populace is safe back in the homeland. Now, the new frontlines of this War on Terrorism are defined by where and when an attack happens; the new soldiers are America's first responders. Unfortunately, as 9-11 demonstrated, these new frontline "warriors" do not fully possess the tools, training, or most importantly, the interoperability that their military counterparts have perfected over the past several decades.

Among these tools, communications capability represents the most important force multiplier on the battlefield. For the first responder, communications capability is absolutely essential. One emerging communications and data-sharing tool that can greatly empower first responders, and provide them with greater situational awareness and "decision superiority," is Peer-to-Peer Technology (P2P). P2P technology allows two or more computers to establish direct contact without a central entity. Such technology provides a rapidly established, flexible, and dynamic architecture. Moreover, it provides a robust, reliable, and distributed information-sharing capability for homeland security applications.

US Northern Command (USNORTHCOM) represents the Department of Defense's (DoD's) operational command for Homeland Security. One of its key missions is to

provide military assistance to civil authorities, including consequence management operations during terrorist attacks. This research will explore and advocate using Peer-to-Peer (P2P) technology within USNORTHCOM and Homeland Security architectures to enable the creation of an interoperable, flexible, and robust communications and data-sharing network. The primary objective of this research is to determine how P2P technology can improve homeland security crisis-response elements to benefit first responders and their respective agencies. Further, it seeks to explore how USNORTHCOM can leverage P2P technology to facilitate DoD's role in consequence management.

Chapter 1

Introduction

Communications dominate war, broadly considered, they are the most important single element in strategy, political or military.

Alfred Thayer Mahan
US Naval Institute, 1900

Radio channels were initially oversaturated and interoperability problems among jurisdictions and agencies persist.

Arlington County After Action Report
on the Response To the Attack on the Pentagon, 9-11

When the next war starts, no one will be fully prepared. As Sir Michael Howard, an esteemed British military historian once said, "Usually everybody starts even and everybody starts wrong… the advantage goes to the side which can most quickly adjust itself to the new and unfamiliar environment and learn from its mistakes."[1] In today's Global War on Terrorism, this now applies as much to a soldier in Iraq as to a law enforcement officer anywhere in the United States. Front lines, defined solely by the geographic placement of military forces, no longer exist. The events of September 11, 2001 (9-11), prove that the battleground is truly global and terrorists can strike Americans anywhere – even within the homeland.

The New Front Lines

Since the end of the Cold War, the US military has committed significant resources and devoted tremendous effort to develop new doctrinal approaches to ensure US military dominance. Specifically, the US military continually works to innovate and improve the tools available to the information age warrior. These improvements aim to bring about decision superiority—to equip warriors and leaders with the right information at the right time to make the right decisions.[2] Progress is especially evident in the areas of communications and information sharing. Now, the US must leverage the advances in military-applied technology to enable first responders fighting here at home. The soldier's toolkit must become the first responder's toolkit.

Unfortunately, the current information sharing and communications architectures do not provide first responders with the necessary capabilities. Virtually every after-action report from 9-11 highlighted the lack of interoperability as the number one shortfall among first responders. Critical information did not reach the right people at the right time and first responders could not communicate effectively amongst themselves.[3] Over 300 firefighters died in the World Trade Center towers because they were unable to receive evacuation warnings coming over police radios. Fortunately, emerging technologies offer solutions to these problems.

The primary objective of this research is to determine how Peer-to-Peer (P2P) technology, can improve homeland security crisis-response elements to benefit first responders and their respective agencies. Further, it seeks to explore how US Northern Command (USNORTHCOM) can leverage P2P technology to facilitate DoD's role in consequence management.

Peer-to-Peer Technology

In the spring of 2000, P2P technology took the Internet computing world by storm. First popularized by a music-sharing software called Napster founded in May 1999, the number of P2P companies grew from zero to fifty in less than 12 months.[4] P2P technology made headlines when, in August 2000, Intel Corporation announced that it was taking the lead and establishing an industry-wide working group to advance infrastructure standards for peer-to-peer computing.[5]

Hailed as the next Internet revolution, P2P advocates pointed to the early 1990s when a program called Mosaic allowed people to "browse" the Internet. This browser led to an explosion in web servers from fewer than 50 in 1992 to over 10,000 in 1994. Similarly, P2P technology proponents predict that with standard P2P protocols, another revolution in capability is just around the corner.

P2P computing is defined as the sharing of computer resources and services by direct exchange.[6] At first glance, that does not sound very revolutionary. However, in reality, it turns the networked world upside down. Currently, most networks are designed with large and powerful servers as "hubs" for information and control. These servers are powerful computers that do the "heavy-lifting" by providing storage, printing capabilities, or network control. In a classic architecture, servers exist to support "clients" that are out at the "edges" of a network. Clients may be personal computers (PC), workstations, personal digital assistants (PDAs), printers, or sensors that use the server as central hub for resources, such as files, devices (like printers), and even processing power.[7] (See figure below.)

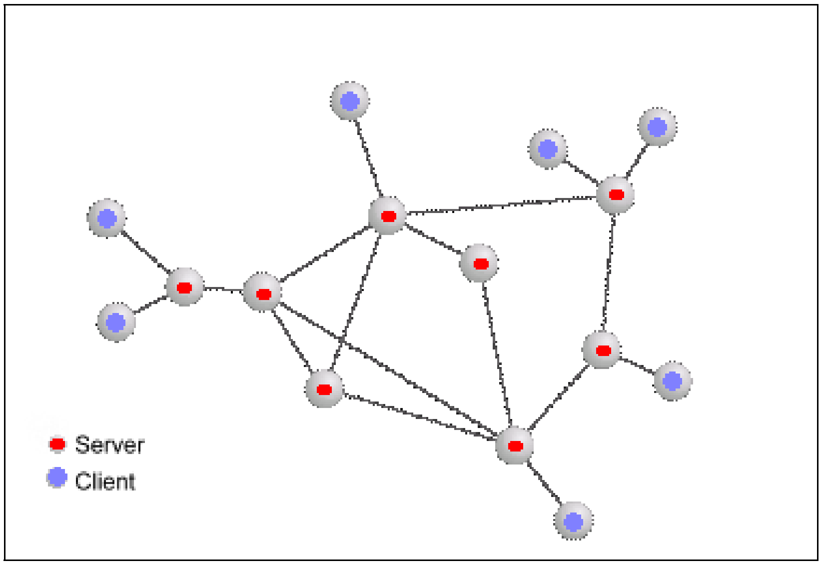

Figure 1. Client-Server Framework

With P2P, clients on a network can simply bypass the server and exchange information over the network directly. This adds value to the edges of a network where the information is being collected and used. (See figure below.)

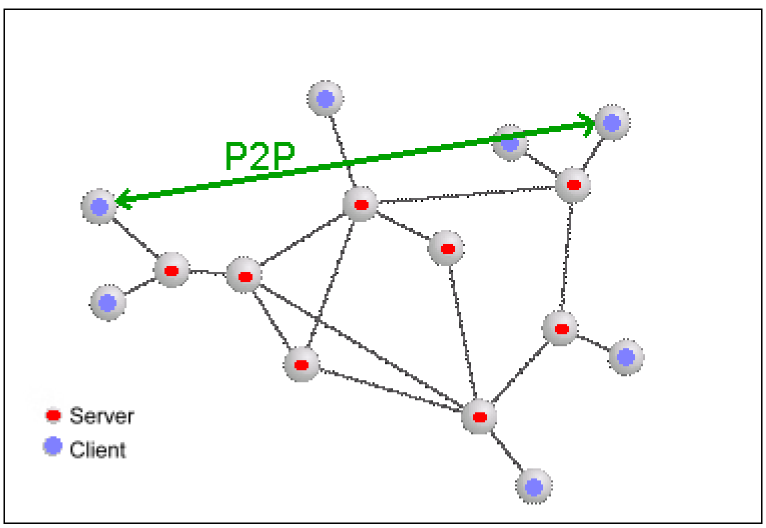

Figure 2. Peer-To-Peer Framework

This paper will provide a basic understanding of P2P technology, as it's evolving in the commercial world. This understanding can serve as a launching point for further comprehension of the information-age possibilities that P2P technology brings such as

the ability to link many different first responders in a secure, robust, reliable and flexible information-sharing network.

P2P and First Responders

The P2P revolution provides a capability to begin solving the interoperability problem between first responders. This thesis explores the various P2P concepts in the commercial marketplace and addresses their potential applicability to homeland security and first responders.

Chapter 2 outlines the extent of the problem and challenges associated with the current lack of interoperability among America's first responders. In addition, the chapter introduces through a case study, some of the ongoing efforts to address this situation.

Chapter 3 defines P2P technology and details how it is deployed over the Internet. It describes various P2P models and describes some of the current P2P technologies at work in the homeland security domain.

Chapter 4 describes the role of USNORTHCOM in providing support to civil authorities. It examines the role that USNORTHCOM plays in consequence management support and describes an ongoing program within DoD to improve information sharing between DoD and first-responder agencies. Chapter 5 explores the possibilities for P2P technology to internationalize information sharing with Canada and others.

Chapter 6 describes some cultural, organizational, and training changes that will be required to allow P2P technology to be deployed to enable first responder communication and collaboration. It will also address some key conclusions and recommendations to make P2P technology more prevalent within the homeland security domain.

Finally, Appendix A offers a notional vignette to help readers better understand the interplay between this technology and first responders. Appendix B provides background information on the organizational roles and responsibilities of the largest homeland security stakeholders. It is recommended that readers unfamiliar with these organizations and their roles read Appendix B before reading the rest of the paper. Appendix C explores the characteristics of robust P2P architecture that will be necessary to realize the full potential of the technology and enable a dynamic information-sharing environment. To provide a more complete description of the benefits and dangers of P2P technology, Appendix D addresses the promises and perils of the technology.

Notes

[1] Sir Michael Howard, "Military Science in an Age of Peace," *Royal United Services Institute for Defence Studies,* March 1974, 6.

[2] Department of Defense, *Joint Vision 2020*, (Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000), 8.

[3] Reports include: "Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon," available from http://www.co.arlington.va.us/fire/edu/about/after_report.htm; "APCO International Homeland Security White Paper," available from http://www.apcointl.org/about/ Homeland/homeland.html; and the "McKinsey Report - Increasing FDNY's Preparedness" available from http://www.nyc.gov/html/fdny/html/mck_report/toc.html. All reports accessed on 24 Feb 04.

[4] "Peer-To-Peer Computing," *Peer-To-Peer Working Group*, Adobe Acrobat Document, 10; on-line, Internet, 8 February 2001, available from http://www.peer-to-peerwg.org/specs_docs/collateral/P2P_IDF_Rev1.11-web.pdf.

[5] "Welcome," *Peer-To-Peer Working Group*, n.p.; on-line, Internet, 8 February 2001, available from http://www.peer-to-peerwg.org/index2.html.

[6] Ibid.

[7] "Client/Server Architecture," *zdwebopedia*, n.p.; on-line, Internet, 8 February 2001, available from http://www.zdwebopedia/TERM/c/client_server_architecture.html.

Chapter 2

The Problem

> *Communication at the scene was challenging. Radio traffic overwhelmed the system to the extent that foot messengers became the most reliable means of communicating.*
>
> Arlington County After Action Report
> on the Pentagon Attack after 9-11

This chapter focuses on illuminating the challenges and problems identified during the introduction, namely communicating relevant data to and between first responders in a timely and secure manner. It also addresses the need to enhance interoperability among the disparate agencies responding to emergencies, especially in light of the threat of high-end terrorist attacks. It should become clear to the reader just how large scale, immediate and integral to national security this problem is, and how close, or far away, America is to solving this problem.

The Importance of Interoperability

Just as Desert One, in 1979, was a watershed event for US military interoperability, or lack thereof, the events of 9-11 have become the interoperability watershed event for first responders across North America. Similarly, just as there was both a plethora of documentation regarding a lack of first responder interoperability prior to 9-11, and a corresponding amount of disparate effort put into addressing it, it still took a singularly

disastrous event, namely, the death of over 300 firefighters whose radios could not receive police warnings who got trapped in the collapsing towers, to focus a spotlight on this situation.[1] Despite three and a half years work on homeland security and billions of dollars spent, the first responder communication situation is still not much better. Representative Jane Harman, a California Democrat who has taken the first responder interoperability challenge head on in Congress states, “We are nowhere--repeat, nowhere--on interoperability.”[2] Although some consider Harman’s comments extreme, no one would disagree that first responder interoperability is of prime concern for homeland security. The world’s leading law enforcement organization, The International Association of Chiefs of Police (IACP), lists improving information sharing and first responder communications among its three priorities for law enforcement in 2004. In his annual address, the IACP’s new president and Chief of Police for Garden Grove California, Joseph M. Polisar, confirmed this sentiment by saying, “…of critical importance in the coming year will be the coordination of our efforts to promote better information sharing among law enforcement agencies…. Just as important is our ability to communicate with one another.”[3]

The Problem

The idea of first responder interoperability is not new. Agencies from jurisdictions that share a boundary have always recognized a need, if not a means, to communicate with one another, especially as the level of an emergency increases with a corresponding increase in the number of responding agencies. In other words, interoperability is most needed at the most critical times; and, its failure can lead to even more catastrophic consequences. In its 2003 Homeland Security White Paper, the Association of Public-

Safety Communications Officials International (APCO), the world's oldest and largest professional organization dedicated to the enhancement of public safety communications, highlighted the importance of interoperability during those incidents that are the most catastrophic. (See figure below.)

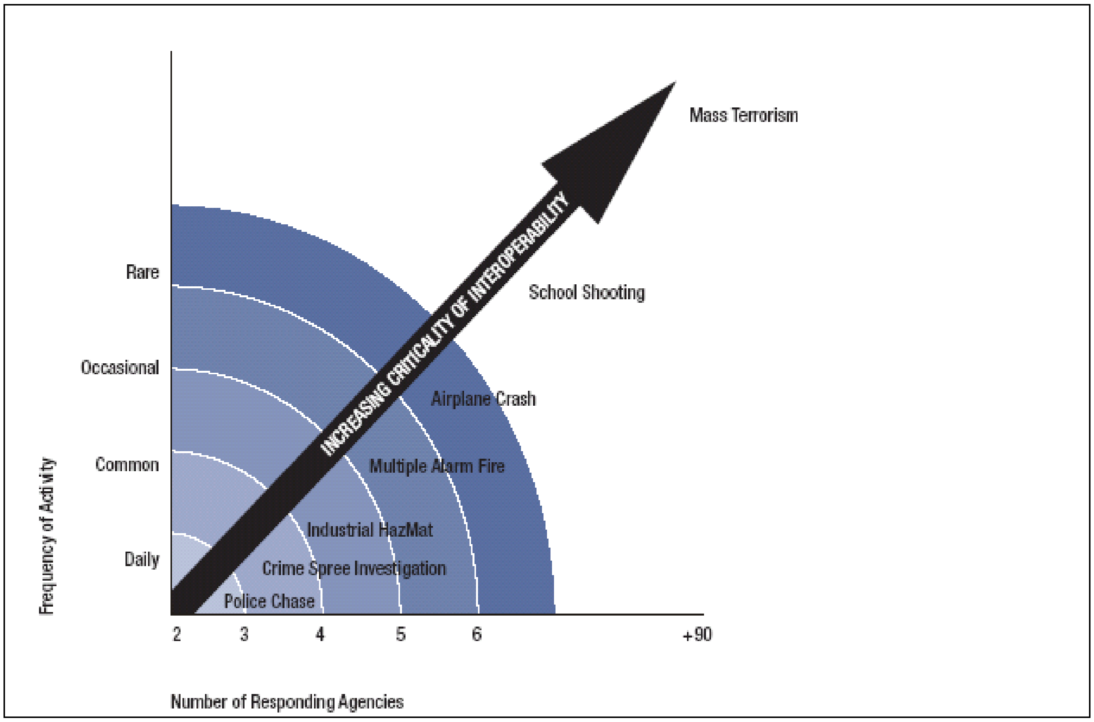

Figure 3. Criticality of Interoperability[4]

Historically, first responders rarely required a high degree of interagency interoperability; therefore, similar to the former military situation, money and effort had not been allocated to solving this problem. In fact, over ten years ago, after the first attempt to topple the World Trade Center failed, the then NYFD Chief of Fire and Rescue Operations highlighted the need for an "…integrated system to link first responders" in his post incident comments.[5] The need went unmet. Similar to the US military response after Desert One in 1979, only uncoordinated and sometimes half-hearted efforts were put forth to remedy this situation. For the US military, this contributed to interoperability

problems noted in both the 1983 Grenada and 1991 Persian Gulf operations. Indications from the recent Iraq War show evidence that these problems are being overcome as interoperability and "jointness" reigned supreme.[6] For first responders, it appeared that a similar trend of interoperability failures would continue until the "pain" became so severe that it could no longer be tolerated or ignored. It appears that pain threshold was reached on Sept 11, 2001.

Increased Urgency

Since 9-11, the sheer magnitude of that tragedy, combined with a renewed sense of urgency by powerful stakeholders like Congresswoman Harman, has resulted in a lasting focus on interoperability and data sharing that appears to be making a difference, and, if pursued to completion could achieve "jointness" in the civilian world. Leading this effort are several governmental and private organizations led by DHS. DHS, as the responsible lead federal agency charged under the Homeland Security Act of 2002, is tasked with,

> Coordination and sharing of information related to threats of domestic terrorism, within the department and with and between other federal agencies, state and local governments, the private sector, and other entities.… It also must share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.[7]

More specifically, the Emergency Preparedness and Response Directorate (EPR) within DHS, "is responsible for building a comprehensive national incident management system with federal, state and local governments…. Further, EPR is to develop comprehensive programs for developing interoperable communications technology and helping to ensure emergency response providers acquire such technology."[8] Despite these congressional mandates, DHS, being a brand new organization, was not positioned

to fully implement them. Therefore, for the past two and a half years, regional and local organizations have moved ahead independently.

Although these independent effort may not result in a unified, coherent national system, it did allow the end users to “home grow” their own systems instead of having them mandated by an outside federal agency, a situation that had led to problems in the past.[9] More importantly, it allowed regional and local agencies time, the impact of which cannot be overstated. Many agencies took advantage of this time to properly research, test and develop interoperable data sharing and communications systems that are now becoming the backbone of a national, interoperable communications network. Additionally, considering that America had recently been attacked, multiple, independent regional programs were not susceptible to another “single” information attack. Therefore, ad hoc redundancy was achieved whether planned for or not, a feature that would have to be integrated into any future national system.

CapWIN Case Study

One of these regional programs, the Capital Wireless Integrated Network (CapWIN) project, formed in the Virginia, Maryland, and District of Columbia area, provides a classic example of how local agencies were able to capitalize on this time to develop a viable interoperable solution. CapWIN is one of the pre-9-11 communications interoperability programs that grew out of an incident that occurred in 1998 when a deranged individual tied up traffic in the metro D.C. area for hours.

> On November 5, 1998, an armed man climbed onto the railing of the Woodrow Wilson Bridge. For the next five hours, he held police at bay, until he ultimately plunged into the river and was rescued. This incident tied up the Capital Beltway for hours causing traffic backups of up to twenty miles. During the incident, police, fire, emergency medical service, and transportation officials from the District of Columbia, State of

> Maryland, and Commonwealth of Virginia, as well as Alexandria City and several federal agencies responded. The resulting traffic problems affected numerous other agencies and jurisdictions throughout the Washington, D.C. metropolitan area. *It was clear during this incident that these multiple agencies from various jurisdictions had no effective way to communicate and coordinate with each other (authors' emphasis).*[10]

Recognizing the potential for future incompatibility problems, the agencies involved cooperated in a forum to address interoperability and launched CapWIN. The result is a 40-plus agency program with over 10,000 users that technologically acts as a backend communications bridge to enable interoperability. (See figure below.)

District of Columbia	Maryland	Virginia	Virginia	Federal Agencies
Washington Metropolitan Police	Prince George's Co. Police Department	Alexandria City Police Department	Loudoun Co. Fire and Rescue	United States Park Police
District of Columbia Fire and EMS Department	Prince George's Co. Fire and EMS Department	Alexandria City Fire Department	Loudoun County Sheriff's Department	United States Department of Justice/National Institute of Justice
Emergency Management Agency	Montgomery Co. Department of Police	Arlington Co. Fire Department	Prince William County Fire and Rescue	United States Department of Transportation
D.C. Public Works	Montgomery Co. Division of Fire & Rescue Services	Arlington Co. Police Department	Prince William County Police Department	Public Safety Wireless Network
Washington Metropolitan Area Transit Authority	Maryland State Police	Fairfax Co. Police Department	Other Agencies	Federal Bureau of Investigation
Metropolitan Washington Council of Governments	Maryland State Highway Administration	Fairfax Co. Fire and EMS Department	International Association of Chiefs of Police	United States Capitol Police
	Maryland Emergency Management Agency	Virginia Department of Transportation	International Association of Fire Chiefs	Federal Protective Service
	Maryland Institute for EMS Systems	Virginia State Police	National Institute for Missing Children	
	Prince George's Co. Department of Public Works	Department of Emergency Management	** Richmond Virginia Region* **Baltimore Maryland Region*	
	Montgomery Co. Department of Public Works	Virginia Emergency Medical Services	** Interested in becoming part of CapWIN*	

Figure 4. CapWIN Participants[11]

CapWIN's Director, George Ake describes it as "A vision for the first multi-state wireless integrated network. This network is built on partnerships and will stand as a model for the country."[12] By examining the CapWIN timeline, the reader can visualize the detailed planning and implementation that went into this project. (See figure below.)

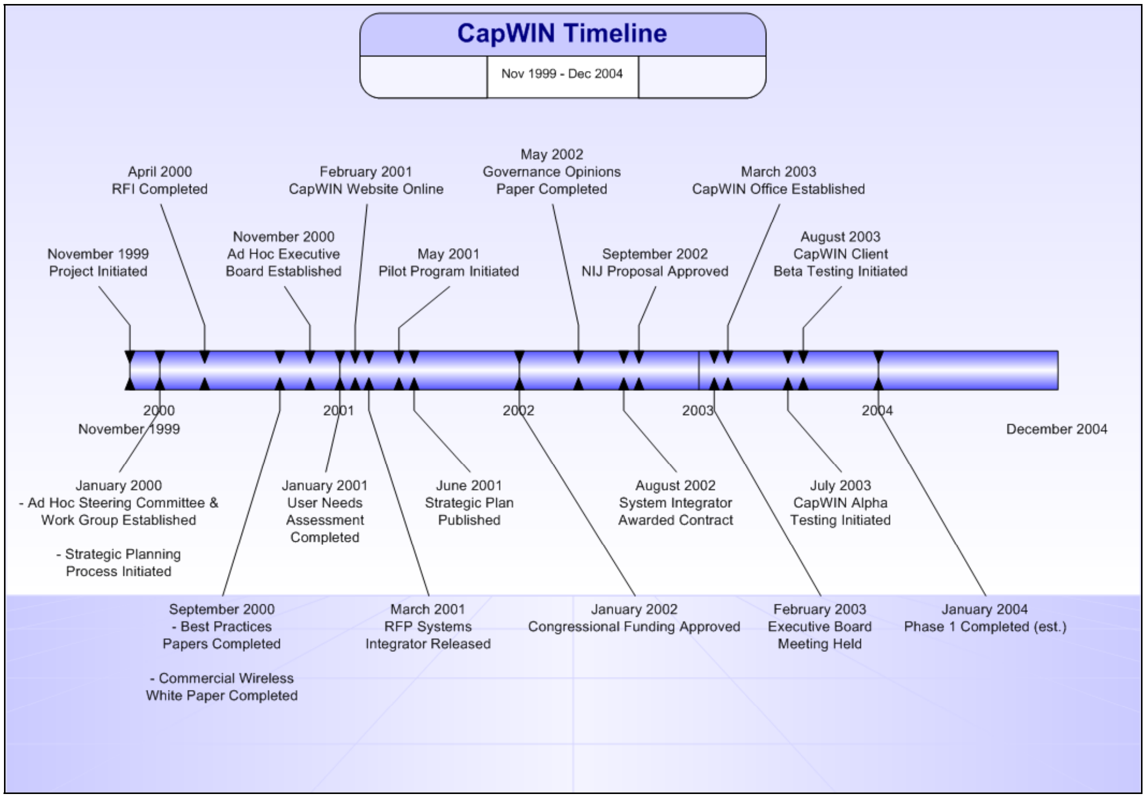

Figure 5. CapWIN Timeline[13]

At the start of this endeavor, CapWIN conducted a thorough user needs assessment, an essential beginning step to any successful problem-solving operation. The assessment asked the end users to identify and answer all of the who, what, where, when, and how questions of first responder data sharing and interoperability.[14] The IACP, in conjunction with the University of Virginia, School of Engineering and Applied Science was selected to conduct the CapWIN assessment.

Not surprisingly, the study revealed some intuitive and already well-established truths among first responders across the spectrum of professional specialties. First, on a daily basis, there is a substantial (more than half) amount of multi-jurisdictional, multi-disciplinary incidence response and the current disparate communications systems in place are inadequate for the task of handling this interaction in an efficient or effective

manner. Second, most communication between first responders is conducted verbally and, more often than not, involves multiple echelons of "message transmitters," read dispatchers, who filter and exchange that information. Each of these re-transmissions of data increases the opportunity for "message distortion," especially in crisis situations. Third, because agencies are locked into using their respective legacy communications systems, which contributes to stovepipe information flow, there is a significant redundancy of effort when multiple agencies compete to accomplish similar operations. Fourth, first responders are cut out of the information processing loop which usually ends up being conducted by a dispatcher and some 3rd party organization/agency. Again, this increases both the chances for communication mistakes and the time necessary to "respond, handle, and clear incidents."[15] The IACP/University of Virginia report concludes by stating,

> As it stands, there is currently a deficiency in the ability for law enforcement to exchange timely data with each other and with other disciplines. This has a less-than-acceptable end result in stale information, crucial information that is never exchanged, wrong information that is exchanged, and redundancy in efforts of incident handlers. The public price for this is longer incident clearing. The private price for this could be the sacrifice of life by a public service provider. The CapWIN system can provide a link that can resolve this issues[16]

This needs assessment mirrored others conducted across the nation and reinforced the requirement for first responder data sharing and communications interoperability. Moreover, it clearly demonstrated the need for first responders to communicate directly to other first responders and to multiple real time sources of information critical to the incident at hand without the intervening "dispatcher" levels of interference.

The Challenge of Limited Bandwidth

Radio communication tools require large amounts of frequency bandwidth. The more radios you add, and the more they are used (as in a crisis situation), the more bandwidth they require. Unfortunately, in this context, bandwidth is a finite resource. Moreover, many jurisdictions have already reached the limits of their bandwidth and this has already caused incidence response problems. Despite efforts to give first responders more bandwidth by allocating former commercial TV frequencies to them, most agencies project using up this new bandwidth almost immediately upon its allocation.[17] From a military perspective, bandwidth is just as problematic. The commander of US Strategic Command, Admiral James Ellis, stated in 2003, "The US military needs a bandwidth appetite suppressant…. We're like kids in a candy store. If it's there, we'll use it."[18] Therefore, both the military and civilian communities need to find new avenues to use bandwidth more effectively. One way to address this is with Internet protocols that offer much greater potential to use limited bandwidth. Furthermore, the Internet offers a solution to the interoperability problem as well.

A key emerging technology that can enable both interoperability and make better use of limited bandwidth is P2P technology. Interestingly, in December 2003 the Department of Homeland Security announced its choice for a nationwide terrorist pre-attack planning and post-attack response, communications and data sharing system. Their choice was JRIES, the Joint Regional Information Exchange System, a P2P network using a program developed by Groove Networks, the same collaborative tool the authors used to research and write this paper while stationed in two separate countries. The following chapter will

explain P2P technology and how it can be used in the homeland security environment to empower first responders.

Notes

[1] Alice Lipowicz and Tim Starks, “Can We Talk? Not Yet, Says an Angry Jane Harman, Targeting Emergency Radio Systems,” Congressional Quarterly, Homeland Security/Technology, n.p., on-line, Internet, 6 November 2003, available from http://www.cq.com.

[2] Ibid.

[3] Joseph Polisar, “Global Leadership in Policing,” The Police Chief, v. LXX, number 11, November 2003, 6, 8.

[4] Association of Public Safety Communication Officials (APCO) International “Homeland Security White Paper,” 8, n.p., on-line, Internet, 27 February 2004, available from http://www.apcointl.org/about/gov/HSTFWP.pdf.

[5] Dawn S. Onley, “First Responders Could Get Access to Military Technologies,” Government Computer News, n.p., on-line, Internet, 17 September 2003, available from http://www.gcn.com.

[6] Personal observations on these three conflicts

[7] United States General Accounting Office, Testimony Before the Committee on Government Reform, House of Representatives, “Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues,” Statement of Robert F. Dacey, Director, Information Security Issues and Randolph C. Hite, Director Information Technology Architecture and Systems Issues, GAO-03-715T, 8 May 2003, 1-2.

[8] Ibid, 17-18.

[9] Richard Jaehne, Illinois Fire Services Institute, interview, Champaign, Il, 26 Sep. 2003.

[10] “A Study of Best Practices in Information Integration Projects,” Capital Wireless Integrated Network Demonstration Project (CAPWIN), 1, n.p., on-line, Internet, 27 February 2004, available from http://www.capwin.org/extras/reports/Best_Practices.pdf.

[11] Capital Wireless Integrated Network, “CapWIN Master Overview Presentation,” 27 June 2003, 26, CD-ROM, CapWIN, 4 December 2003.

[12] Ibid, 18-19.

[13] Ibid, 21.

[14] These include: Who are all the first responders? What information do they require? Who do they need to communicate with? When do they need to communicate? How can and should they communicate?

[15] International Association of Chiefs of Police & The Center for Transportation Studies, School of Engineering and Applied Science, The University of Virginia, “The Capital Wireless Integration Network (CapWIN) Project An Assessment of Select Metropolitan Washington Public Safety and Transportation Agencies User Needs,” February 2001, 79-95, n.p., on-line, Internet, 27 February 2004, available from http://www.capwin.org/extras/reports/user_needs_assessment.pdf.

[16] Ibid, 104

Notes

[17] Peter Roy and Joe Ross, Office of the Chief of Technology, D.C. Metropolitan Police Department, interview with authors, Washington D.C., 4 December 2003.

[18] Jason Bates, "US Commander Warns Military," *Defense News*, 15 September 2003, 52.

Chapter 3

P2P Technology and First Responders

If a million people use a Web site simultaneously, doesn't that mean that we must have a heavy-duty remote server to keep them all happy? No; we could move the site onto a million desktops and use the Internet for coordination. Could Amazon.com be an itinerant horde instead of a fixed Central Command Post? Yes.

David Gelernter
The Second Coming—A Manifesto

Consider what is located at the edges of a first-responder network—firefighters, law enforcement, medical personnel, hospitals, HAZMAT teams, public health and intelligence teams. Imagine the possibilities if first responders could link directly to each other and tap into the wealth of information available through the Internet. Imagine the possibilities of linking first responders to each other, criminal databases, HAZMAT databases, and dedicated science teams to build an accurate picture of the area of operations not only in some incident command center miles from the incident, but also in the hands of the front-line first responders. The proliferation of wireless communications and computers in the hands of first-responders continues unabated. Many squad cars in major metropolitan areas carry a wireless-networked laptop computer.[1] Many software vendors are developing handheld Personal Digital Assistant (PDA) software for first responders – many of which will wirelessly share information with other authorized users

within range.[2] P2P technology could leverage these systems to make everything a peer—linking first-responders, sensors, intelligence teams and decision-makers.

As illustrated in chapter 2, the flow of information between first responders is hampered by a traditional hierarchical data flow and "stove-piped" systems. In most cases, if cross-jurisdictional communication must take place, it must be "controlled" on a case-by-case basis by the dispatchers from each jurisdiction. Dispatchers routinely relay messages between first responders verbally or manually patch them through to each other.[3] It would be far better for our first responders to communicate directly with each other without the hierarchical "control."

P2P technology offers more than a way to link first responders. It presages a new way of thinking about how to take advantage of the information and intelligence that reside at the edges of a network. For example, most organizations have well defined processes and procedures. These hierarchical, centralized, and repeatable processes evolved to enable the organization consistently to meet its objectives. However, when an "unusual" or unanticipated crisis arises, the organization must adapt. Ad-hoc, spontaneous, and agile teams form to address the new situation. Such dynamic and adaptable solutions draw greatly on the intelligent people and their information at the edges of a network. P2P technology enables edge-based organizational adaptability by providing tools for teams to form quickly and efficiently.

A basic understanding of P2P technology, as evolving in today's business environment, can serve as a launching point for further understanding of the information age possibilities that P2P technology brings to first responders.

What is P2P Technology?[4]

P2P is defined as "A network where there is no dedicated server. Every computer can share files and peripherals with all other computers on the network, given that all are granted access privileges."[5] Alternatively, it can also be defined as, "A communications network that allows all workstations and computers in the network to act as servers to all other users on the network."[6]

P2P technology has been enabled by significant changes in the capabilities of the average desktop and laptop PC. The average PC now has the same computing power and hard-drive storage that only a server could have just a few years ago. Furthermore, the advent of cable modems and digital subscriber lines (DSL) has allowed PCs to receive and transmit high volumes of information.[7] "What has changed is what the nodes of these P2P systems are—Internet-connected PCs, which had been formerly relegated to nothing but clients—and where these nodes are—at the edges of the Internet."[8] Thus, the real impact of P2P technologies is that they are "leveraging previously unused resources."[9] These resources on the Internet are hundreds of millions of people and their PCs, laptop computers, PDAs, IP Radios, cell phones and other devices. Moreover, the explosion in wireless capabilities and connectivity allows virtually any device to be networked to another device without a "hard-wire" connection.

However, one of the major challenges of P2P technology lies in the transient nature of these resources. Up until 1994, the Internet connectivity model assumed that the nodes were always on and always connected.[10] Large servers run by universities and businesses were the main nodes, were always on, and operated as peers. However, with the invention of the web browser, in the early 1990s, and the subsequent explosion of web

sites to serve consumers around the world, more people used a modem to connect their PCs to the Internet through telephone lines. With the growth of consumers wanting to connect to the Internet, Internet Service Providers (ISPs), such as America On-line and CompuServe, rushed to meet the demand. ISPs offer a phone number that allows a user's PC to link with a large server that links to the Internet. Once connected, a PC is assigned a temporary Internet Protocol (IP) address. This address allows servers to send and receive information to and from each PC. These PCs go “on-line” for relatively short periods of time and would enter and leave the network cloud frequently and unpredictably.[11] Furthermore, ISPs typically assigned a different IP address when the PC came on-line. Thus, information housed on a PC could never be consistently addressed and it was virtually impossible to know with any level of certainty who was at a given IP address. As a result of these transient connections and limited computing power, PCs were relegated to lower-class status compared with the “heavy-lifting” servers.

P2P technology has changed the limitation of transient connections by establishing a method to deal with the nature of people who are always coming and going at the edges of the network. They do this by indexing “pseudonyms.” Therefore, when a user connects, his IP address can be updated in real-time. For example, many popular P2P programs require a user to create a pseudonym or username when they first sign on. This pseudonym identifies the user, not a specific device with a specific IP address. When a user signs on to the P2P service, the service checks its pseudonym database and links the user and his current IP address. Thus, the P2P service overcomes the limitation of constantly changing IP addresses by creating a central index or database so that people

can connect to each other through pseudonyms. This ability to overcome the transient connection limitation gives P2P the ability to "handle unpredictability, and nothing is more unpredictable than the humans who use the network."[12] First responders at an incident will fit this model exactly. They would be best described by an ever-changing network cloud of users entering and exiting the network. All of them enabled by a combination of hardwired, wireless and Radio Frequency communications.

The network exists to serve the humans and other devices at the edges of the network and the continuing challenge has been to make the network more people friendly. With the increase in computing power and connection speed, PCs and other devices now can operate as nodes like servers had in the past. On any network, value is added to the information through the nodes at the edges of a network. This is where people or sensors add intelligence to the information to increase (or decrease) the information's value. However, until recently, the information at the edges was largely inaccessible. Instead of moving or copying this valuable information to a central, shared server, P2P moves the server to each of these devices.[13] Thus, a P2P network takes advantage of the "intelligence" at the edges of a network by allowing them to link together directly without the "controlling" influence of a central server.

The fact that just about any device can now connect to the Internet and serve as a node is a radical departure from the previous client-server mindset. The network, which was previously dominated by large resource-rich processors, is now populated by a variety of smaller devices ranging from laptops to personal digital assistants to cell phones to embedded controllers.[14] Gene Kan, one of the original developers of the Gnutella P2P communications protocol writes, "Tomorrow's applications will take this

infrastructure for granted and leverage it to provide more powerful software and a better user experience in much the same way modern Internet infrastructure has."[15]

Back to the Future: The History of the Internet[16]

In many ways, the advent of P2P takes the Internet back to its roots as a true P2P system. In the early 1960s, the RAND Corporation began research into robust, distributed communication networks for military command and control. The Department of Defense's Advanced Research Project Agency (ARPA) built the first ARPANET by linking four universities in 1969. ARPANET treated each node as an equal and linked them together as peers rather than in a client-server relationship.[17]

The original application that overtook all competitors, also known as a "killer app," was e-mail.[18] This application was very popular because it enabled researchers to collaborate on scientific endeavors. Twenty-three universities and government research centers were connected on ARPANET by 1971. Throughout the 1980s, parts of the original ARPANET were commercialized and the Internet expanded from 200 to 60,000 nodes. Furthermore, software developed that quickly became the common language of all Internet computers and allowed two-way communication between nodes. In the mid-1980s, the formation of the Internet Advisory Board and the Internet Engineering Task Force (IETF) served a critical function by providing a forum for designers, operators, and researchers to collaborate and incorporate "best standards for protocols and procedures."[19] One primary example of a protocol promoted by the IETF is the Hyper-Text-Transfer-Protocol (http) that begins virtually every web address. The late 1980s witnessed the first major security attacks and the establishment of the Computer Emergency Response Team (CERT) to address security concerns across the Internet.

Throughout the 1980s, federal agencies shared the cost of a common infrastructure and managed “interconnection points.” The National Science Foundation (NSF) encouraged its regional networks, primarily academic institutions, to pursue commercial customers to use their networks and lower funding for all. The NSF restricted use of their networks to “Research and Education Only,” which encouraged the growth of private, long haul communications infrastructure that became the foundation for today’s information superhighway. All of these decisions created a vast network of networks that led to the decommissioning of ARPANET in 1990.[20]

The 1990s saw the most explosive growth of the Internet. In 1991, the NSF raised the restrictions on commercial traffic across the NSFNET Internet backbone. In 1993, the first “web browser” became available which enabled average computer users to browse the web. This led to an explosion of Internet use and traffic on the Internet expanded at a 341,634 percent annual growth rate. By 1996, there were over 10 million nodes with over 40 million people connected to the Internet.[21] In 1998, the US Department of Commerce selected a non-profit corporation, the Internet Corporation of Assigned Names and Numbers (ICANN) to function as “the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.”[22]

The original Internet was P2P—with servers acting as clients to other servers and vice versa. The relationship was symmetric and every host on the net could serve any other host.[23] The exponential user growth of the 1990s forced the Internet away from its P2P roots and led to the ubiquitous deployment of the client-server model. Furthermore,

the limited capability of client computers made them more useful as a receiver of information rather than a processor and transmitter of information. As a result, the client-server model surfaced as a way to deal with both challenges. First, the model is simple and straightforward: "the client initiates a connection to a well-known server, downloads some data and disconnects… It just needs to know how to ask a question and listen for a response."[24] Furthermore, if the server is safe from security problems, then the client can also be protected. Second, most of the information is transmitted "downstream" to the user and thus most of the communication "pipes" have more downstream than upstream throughput. This downstream paradigm is being challenged by the P2P revolution where client computers may need to send large quantities of information just like the "heavy-lifting" servers.

P2P Models

P2P technology can be divided into two major categories or models. These models are Broker and No-Broker. Depending on the application of the technology, these models may be combined to yield an optimal solution. Thus, the key components of each can be merged to best fit the situation in which it would be used.

Broker Model

The first P2P application to hit the Internet and receive widespread use was the music-sharing program called Napster in May 1999. Written by a 19-year old college student, Napster instantly met a need and grew to over 40 million users in two years.[25] The program was shut down in 2001 as a result of several successful lawsuits by the Recording Industry Association of America. Napster recently (November 2003) restarted

operations as a legal, more controlled, pay-for-music service. However, the capability has been demonstrated and has been copied by countless other P2P services.[26]

The Napster concept is simple and perfectly illustrates the Broker model. When on-line and using the Napster program, users registered their song files with a Napster server (www.napster.com). Napster then allowed other users to query their server that serves as a central index of registered files. When a user was looking for a song, it queried the Napster central server to discover what other users, currently using Napster, had that specific song file. Armed with that information, the user was then free to link directly to the other Napster user and copy the song file directly from their hard drive. Napster was the Broker that provided visibility from the requestor to the source. (See figure below.)

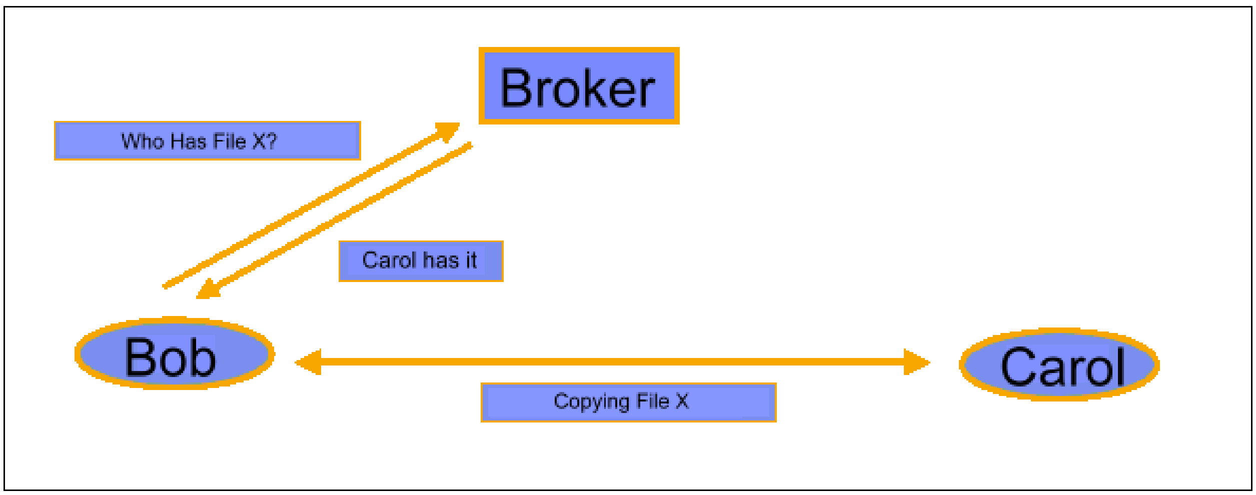

Figure 6. Broker Model[27]

While not completely decentralized, Napster combines just enough centralization to get the job done. Once users become aware of each other, Napster shifts control of the file transfers to the users. Each user had access to gigabytes of songs and was virtually connected to tens of thousands of other users.

There are three dominant strengths of the broker model. First, the central server index minimizes search traffic to find a specific file. With the central server, users only need to query one source rather than searching through all of the users on the network. Second, the broker provides some level of accountability by forcing users to register their files on the central server. Third, the central server can function as the most up-to-date source for information and when new information becomes available, only one index must be updated.

The primary weakness of the central server mirrors its primary strength—centralization. With a central server or servers to make the entire system work, it is certainly vulnerable to physical or information attacks. Another way to think of the central server is as a "single-point of failure." Thus, if it were disabled, the entire system could be rendered inoperable. However, this weakness in no way invalidates the power of the Broker model concept that decentralizes the file-sharing task.

No-Broker Model

Soon after Napster's legal challenges began in early 2000, software developers began looking for another way to share files without the central "broker." Within weeks, a small group of developers working for Gnusoft developed the Gnutella communications protocol--a perfect example of the no-broker model.[28]

The no-broker model overcame the most significant limitation of the broker model. In the no-broker model, there is no central server to provide the "index" to all of the other users. Here users register the files that they want to share with their network neighbors. If someone is looking for a file, he/she asks their neighbors if they have it, or if they know someone who does. That request is propagated throughout the network until the

file is found. When found, the requestor is linked with the owner and the file transfer is enabled. (See figure below.)

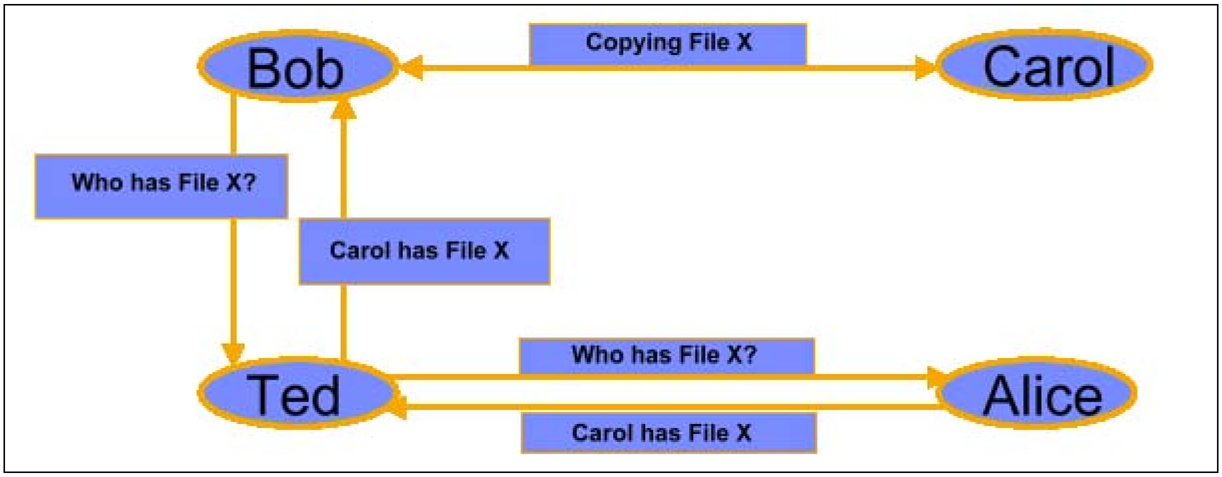

Figure 7. No-Broker Model[29]

A prime example of a decentralized network is the Gnutella network. Developed in 14 days in early March 2000, the Gnutella protocol overcame the central server drawbacks of Napster.[30] "More than just a software program, Gnutella is really an internet built on top of the Internet."[31] As users connect to the Internet, they link-up with other Gnutella users and the network is then created. As each node connects, it brings some network capability that is instantly integrated into the fabric of the network at large.[32] Thus, the physical infrastructure of wires and routers does not change, but which wire and routers participate in the network changes by the second. This makes it a dynamic virtual infrastructure built upon a fixed physical structure.[33] The Gnutella network expands as more nodes connect to the network. Likewise, it does not exist if no users run Gnutella nodes.[34] In Gnutella, every machine in the network is connected to every other machine and no single node is responsible for distributing all of the content. Therefore, if one machine goes down, the network is unaffected, because all the other machines are connected to each other through multiple redundant connections.[35] Another

way to think of Gnutella is like a bucket brigade. "Messages are relayed by a computerized bucked-brigade which forms the Gnutella network. Each bucket is a message and each brigadier is a host. The messages are handed from host to host willy-nilly, giving the network a unique interconnected and redundant topology."[36]

For example, assume that a user is looking for a recipe for strawberry rhubarb pie. Once connected to the network, the user asks its immediate neighbors if they have the recipe. If so, a positive reply is sent to the requestor. Just in case other users might have a better recipe, the user's request is also forwarded to the other nodes in the network. Thus, a large portion of the network is canvassed and many replies are sent to the requesting user.[37] With dozens of recipes to choose from, the user then chooses which recipe he wants and then downloads it from the other users.

There are three strengths of the no-broker model. First, the distributed nature of the network makes it very hard to stop. Without a centralized server (broker) that could be physically, informationally, or legally targeted, it is virtually impossible to shut down such a network. As Thomas Hale, CEO of Wired Planet, said, "The only way to stop Gnutella is to turn off the Internet."[38] Second, the no-broker model is designed to operate with transient connections. This more accurately reflects the way users connect; and, it overcomes one of the significant limitations of the server side of the client-server model that operates best with always-on connections. Third, one of the unanticipated benefits of the no-broker model may be a more intelligent search capability. Traditional search technologies apply only one intelligence to the body of data they search.[39] For example, with Gnutella, each node interprets a user's request differently, which may result in a "richer" set of responses to a specific query. For example, if a user enters "MSFT" each

node may return a different type of answer based on how it interprets the request. In this case, a financial node may return Microsoft's current stock price. A news node may return a list of news stories mentioning Microsoft. Or, a clip-art node might return a graphics file with the Microsoft logo. Thus, the no-broker model has significant strengths that make it a unique capability in the P2P domain.

The weaknesses of the no-broker model stem from its lack of a central server. The “willy-nilly” nature of its searching function makes it inefficient relative to the straightforward broker model. For a no-broker system, a standard search requires high traffic to query the connected nodes. As more nodes connect, more queries are routed throughout the network. This can lead to saturation and an overcrowded network. Second, given the transient nature of the network, sources of information (nodes or hosts) that were “there” the last time a user logged on, may not be available the next time. This drawback relates directly to the ad-hoc nature of the no-broker network. This ever-changing topology of the no-broker model can be major problem if only one node contains the information that a user desires.[40] Third, many of the commercially available no-broker applications build anonymity into their systems. While this may be a benefit to information providers who wish to remain anonymous, users generally evaluate the validity of information by knowing who is providing the information to them. Thus, in many cases, anonymous information transfer is a weakness rather than a strength. Overall, the no-broker model offers some promising capabilities especially by providing an infrastructure for transient nodes to interact directly through a virtual dynamic network.

Hybrid Options

The broker and no-broker models can be combined to create new hybrids that maximize strengths and minimize weaknesses. For example, when the Gnutella network was in its infancy, the only way to find a Gnutella node was by word of mouth. However, users soon became frustrated by the difficulties of getting onto the network. Thus, a program called GnuCache was developed that served as a broker to help users find the rest of the network. This program combined the benefits of the no-broker model with the broker model.

Hybrid systems may also provide a layered Broker capability. For example, the open source community has cloned Napster-like software known as OpenNap. Its Napigator program gives users statistical information about servers that are running OpenNap and allows users to link with the server of their choice. The user can then choose which server to connect with to join an OpenNap file-sharing system.

Current Uses of P2P Technology for Homeland Security

According to the Gartner Group, "P2P is an inevitable evolution for computing."[41] This is proving to be the case in the development of technologies to support first responders. Throughout the US, multiple initiatives will enable direct exchange between first responders.

Capital Wireless Integrated Network (CapWIN)

As mentioned in Chapter 2, the CapWIN program evolved to enable over forty agencies within the Maryland, Virginia and Washington D.C. metropolitan area to communicate directly. It provides a back-end infrastructure that provides messaging, federated database access, and incident management.[42]

Participating agencies are able to communicate with each other via a series of standard devices such as laptops and Personal Digital Assistants (PDAs). Personnel will use these devices to coordinate efforts and to quickly create ad-hoc cross-jurisdictional response teams. A police officer responding to an automobile accident for example, will be able to communicate simultaneously with key personnel including ambulance drivers, firefighters, and transportation response units as well as the hazardous materials team and other special units.[43] The figure below illustrates the logical communications connections that CapWIN enables.

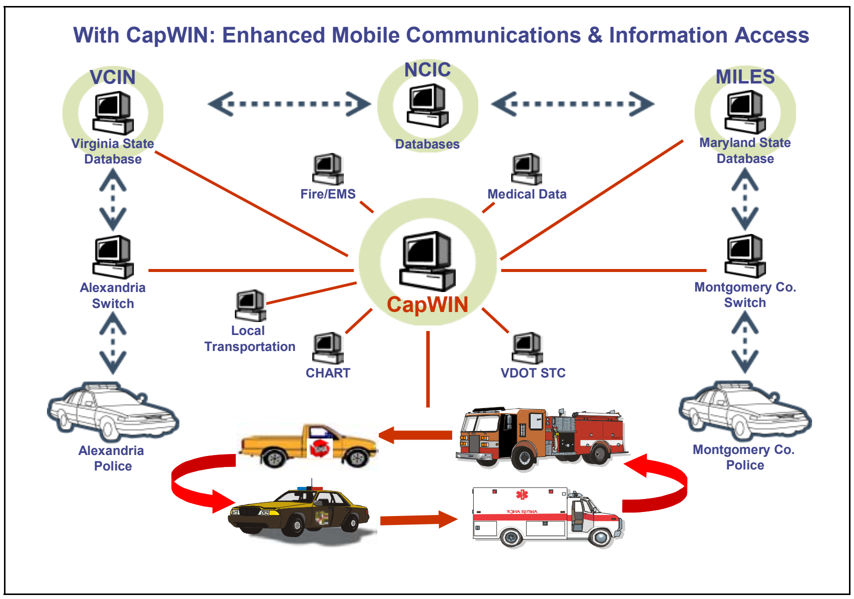

Figure 8. Logical Diagram of Communication Flow Capabilities[44]

CapWIN was designed to allow first responders to communicate directly through their *existing* infrastructure. This use of existing infrastructure is central to the benefit that CapWIN brings, since most jurisdictions cannot afford to regularly purchase new equipment to keep up with the latest technology. CapWIN also provides a way for new users with new wireless technology to easily access the network and its databases.[45] The

figure below illustrates the current architecture for CapWIN and shows the backend infrastructure that enables P2P connections.

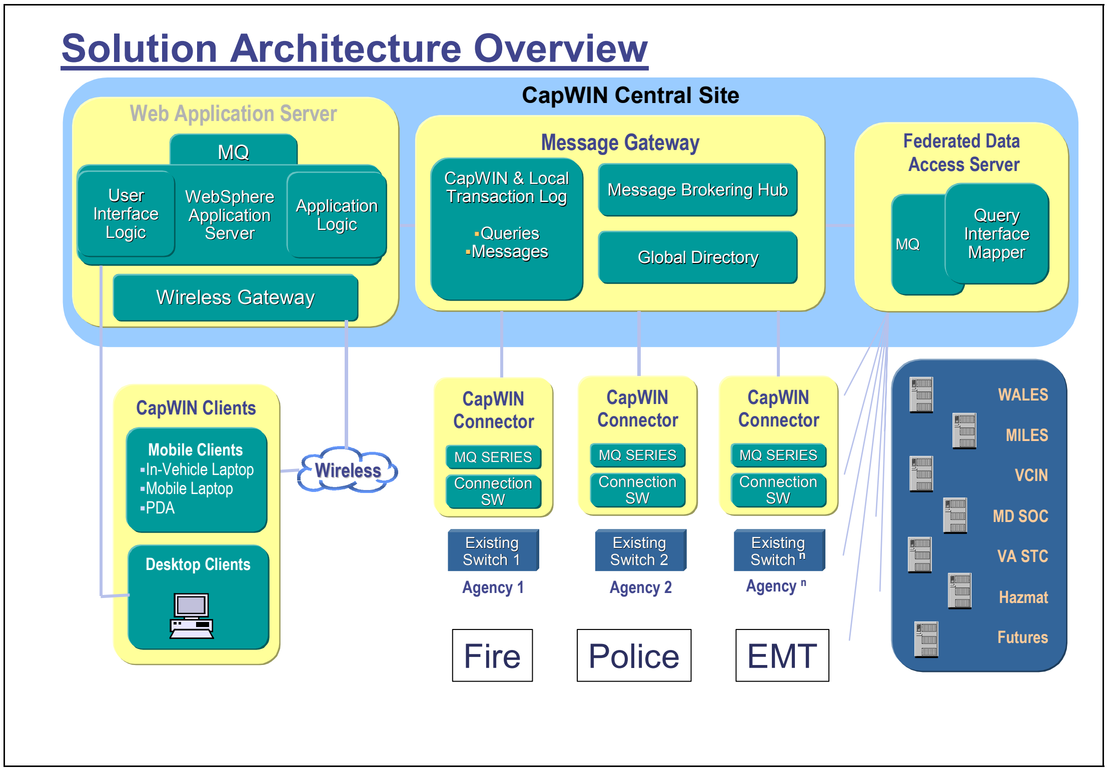

Figure 9. CapWIN Architecture[46]

Joint Regional Information Exchange System (JRIES)

As described earlier in Chapter 2, after 9-11 it was clear to federal, state and local first-responders and public safety officials that they needed a system to share intelligence information between all levels of government. They needed a way to communicate, perform real-time collaboration, and share "sensitive, but unclassified," terrorism information to support threat analysis.[47] Moreover, such a system needed to be relatively inexpensive, quickly deployable, and "partner owned and operated."[48]

A P2P software application was the best choice available to meet the system requirements. Groove Networks' Groove® software provided a relatively inexpensive,

secure, quickly deployable and relatively mature application. It only cost approximately $149 per user and required only a PC or laptop with Internet access. Moreover, it had already passed some critical security certifications for use by the DoD.[49]

The system became known as the Joint Regional Information Exchange System (JRIES). JRIES is currently a primary means of information exchange between hundreds of federal, state, and local intelligence agencies. Moreover, in February 2004, DHS announced the expansion of JRIES to all 50 states, five territories, Washington, D.C., and 50 major urban areas to strengthen its flow of threat information.[50]

Joint Protection Enterprise Network (JPEN)

In June 2002, the Joint Staff embarked on an effort to apply the concepts of network-centric warfare to DoD Force Protection information sharing. JPEN is a rapidly prototyped information sharing system for DoD force protection information. It allows information sharing between DoD facilities. Hosted on a protected network, JPEN is modular and scalable with the ability to upgrade with new technologies and policies. JPEN continues to grow in its capability to link various DoD facilities and provide situational awareness.[51]

JPEN is currently based on a client-server model accessed through a Protected Internet Environment. However, the servers in the system serve as peers to each other to share information.[52] As the system matures, it will provide links for individual users as peers to share information throughout JPEN. The figure below illustrates the current JPEN prototype sites that make up its architecture.

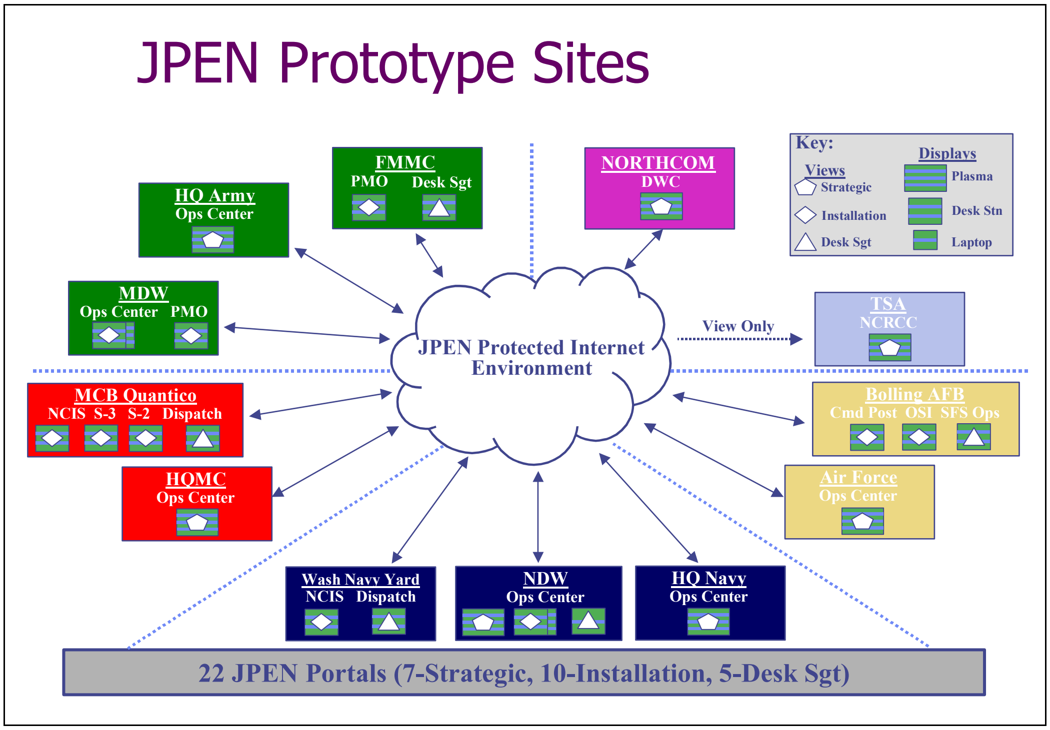

Figure 10. Proposed JPEN Prototype Sites[53]

As elements of the homeland security architecture evolve, they will incorporate more and more P2P technology. The homeland security network will grow to extend beyond links between agencies and operations centers to extend all the way out to the edges of the first responder communities – the first responders themselves.

Conclusion

Peer-to-Peer technology offers dramatic increases in computing power and storage space by empowering and linking the edges of a network. The broker and no-broker models each offer unique capabilities and limitations. The advantages of a P2P network lie in its distributed nature and its ability to handle transient users and devices. Furthermore, linking the various models together may provide more capability than any one model on its own. However, P2P technology is not appropriate in all circumstances. The client-server model, which has served the Internet very well, is much simpler than

P2P and it would not be wise to abandon the simple for the complex without a clear benefit.[54] Ultimately, a combination of P2P with the client-server model will provide first responders with the flexibility and robust information architecture to enable decision superiority.

Notes

[1] "A Study of Best Practices in Information Integration Projects," Capital Wireless Integrated Network Demonstration Project (CAPWIN), 17, 20, 60, n.p., on-line, Internet, 27 February 2004, available from http://www.capwin.org/extras/reports/Best_Practices.pdf.

[2] See PalmOne at http://www.palmone.com/us/enterprise/solutions/government/homeland.security/IatroSoft.html; ePatient Software at http://www.iatrosoft.com/first_responder.htm; and PDAMedic at http://www.pdamedic.com/PdaMedicInfo.htm.

[3] Steve Gluckman, "Capital Wireless Integrated Network (CapWIN): An integrated transportation and public safety information network," *E-Government Executive Education (3E) Project*, John F. Kennedy School of Government, Harvard University, 2003, 2.

[4] Much of the information defining P2P technology and its capabilities was previously published by Major Mark Bontrager, "Peering Into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Distribution and Operational Tasking," (Maxwell AFB, Ala.: School of Advanced Airpower Studies, 2001), on-line, Internet, available at https://research.maxwell.af.mil/papers/ay2001/saas/bontrager.pdf.

[5] "Peer-To-Peer Network," *CNET Glossary*, n.p.; on-line, Internet, 24 February, 2001, available from http://www.cnet.com/Resources/Info/Glossary/Terms/peer.html.

[6] "Peer-To-Peer Network," *Gateway_com Help Glossary*, n.p.; on-line, Internet, 24 February, 2001, available from http://www.gateway.com/help/glossary/glossary_p.shtml.

[7] A modem is a device or program that enables a computer to transmit data over telephone lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms. A cable modem is a modem designed to operate over cable TV lines. Because the coaxial cable used by cable TV provides much greater bandwidth than telephone lines, a cable modem can be used to achieve extremely fast access to the World Wide Web. DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

[8] Clay Shirky, "What is P2P … And What Isn't," O'Reilly Network, n.p.; on-line, Internet, 24 February, 2001, available from http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html.

[9] Ibid.

[10] Ibid.

Notes

[11] Ibid.

[12] Clay Shirky, "Listening to Napster," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 24.

[13] Gregory A. Bolcer et al., *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure,* White Paper *,* (Irvine, CA: Endeavors Technology, 6 December 2000) 6; Internet, available at http://www.endtech.com/news.html

[14] Bolcer, 6.

[15] Gene Kan, "Gnutella," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 122.

[16] The bulk of the information for this section is taken from "Life on the Internet Net Timeline," PBS.ORG, n.p.; on-line, Internet, 24 February, 2001, available from http://www.pbs.org/internet/timeline/index.html.

[17] Nelson Minar and Marc Hedlund, "A Network of Peers," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies,* ed. Andy Oram*,* (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 4.

[18] A *killer app* is an application that surpasses (i.e., kills) its competitors.

[19] "The Internet Engineering Task Force," IETF Web Page, n.p.; on-line, Internet, 31 March 2001, available from http://www.ietf.org/index.html and http://www.ietf.org/rfc/rfc2026.txt.

[20] Barry M. Liener et al., "A Brief History of The Internet, Version 3.31" Internet Society, 4 Aug 2000, n.p.; on-line, Internet, 25 May 2001, available from http://www.isoc.org/internet/history/brief.html#Transition.

[21] "ICANN Fact Sheet," Internet Corporation for Assigned Names and Numbers, n.p.; on-line, Internet, 25 May 2001, available from http://www.icann.org/general/fact-sheet.htm.

[22] Ibid.

[23] Minar and Hedlund, 5

[24] Ibid., 9.

[25] Shirky, "Listening to Napster," 27.

[26] Other Napster-like P2P systems include : Napigator and OpenNap. Other P2P systems that are also widespread include: EarthStation 5, Bit Torrent, Kazzaa, and Limewire.

[27] Adapted by author from original by Bob Knighten, "Peer to Peer Computing," briefing to Peer-To-Peer Working Group, 24 August 2000, 13; on-line, Internet, 11 October, 2000, available from http://www.peer-to-peerwg.org/downloads/collateral/ 200008_IDF/PtP_IDF.pdf.

[28] Kan, 95.

[29] Source: Adapted by author from original by Bob Knighten, "*Peer to Peer Computing*,*"* briefing to Peer-To-Peer Working Group, 24 August 2000, 14; on-line, Internet, 11 October, 2000, available from http://www.peer-to-peerwg.org/downloads/collateral/ 200008_IDF/PtP_IDF.pdf

[30] Kan, 95.

[31] Ibid., 100.

Notes

[32] Ibid., 107.
[33] Ibid., 97.
[34] Ibid., 100.
[35] "What Is Gnutella," *Free Peers Inc.*, 2001, n.p.; on-line, Internet, 25 May 2001, available from http://www.bearshare.com/gnutella.htm#whatis
[36] Kan, 104.
[37] In Gnutella, there is a concept of a horizon. Rather than repeat a request across the network forever, each request is limited to seven hops. Typically, a seven-hops canvasses about 10,000 nodes. (Kan, 110)
[38] Kan, 99.
[39] Ibid., 103.
[40] This would also be a problem in the Broker model if only one node contained the needed information and that node was not available when the user requested that needed information.
[41] J. Sweeney et al., *The Five Peer-to-Peer Models: Toward the New Web,Gartner Group Research Note COM-12-4447* (Stamford, Conn: Gartner Group, February 2001), *3;* on-line, Internet, 21 May 2001, available from http://www3.gartner.com/Init.
[42] Capital Wireless Integrated Network, "CapWIN: Project Solution and Overview April 2003," 9, on-line, Internet, 27 February 2004, available from http://www.capwin.org/extras/reports/CapWIN_Presentation_April2003.pps.
[43] Gluckman, p. 2.
[44] Capital Wireless Integrated Network, 6.
[45] Capital Wireless Integrated Network, 20.
[46] Ibid.
[47] George Marenic, "Joint Regional Intelligence Exchange System," remarks at Government Convention of Emerging Technologies," 8 Jan 04, Las Vegas, Nev.
[48] Ibid.
[49] Ibid.
[50] CQ Press Office, "Homeland Security Launches Expansion of Information Exchange System to States and Major Cities," *Congressional Quarterly, Homeland Security/Technology*, 24 February 2004, n.p., online, Internet, 24 February 2004, available from http://www.cq.com.
[51] US Northern Command, "Joint Protection Enterprise Network (JPEN)," Briefing, 4.
[52] CDR Joel Swanson, USNORTHCOM/J6, interview with Lt Col Bontrager, Colorado Springs, Colo., 13 January 2004.
[53] Ibid., 6.
[54] Andy Oram, ed., *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 396.

Chapter 4

USNORTHCOM and P2P Technology

We don't want to be exchanging business cards at the scene of the incident.

General Ralph Eberhart
Commander, US Northern Command

In today's strategic environment, with the constant threat of terrorist attack, combined with the proliferation of weapons of mass destruction, it is not difficult to imagine an incident that could quickly overwhelm local and regional first responders. Historically, the US military has been called upon to assist when local and regional forces become overwhelmed.[1] To better organize military forces for both homeland defense and homeland security, DoD established US Northern Command (USNORTHCOM) in October 2002.

Heavy Lifter of Last Resort

USNORTHCOM consolidates, under a single unified command, existing missions that were previously executed by other military organizations.[2] By providing much more than a new organizational construct, USNORTHCOM brings unity of command and the alignment of the forces necessary for homeland defense and security under a single four-star commander. This organization now serves as a breeding ground for the synergistic

exploration and implementation of new strategies and concepts to secure the homeland. USNORTHCOM brings the capability to assist with domestic disaster relief operations that occur during fires, hurricanes, floods, and earthquakes. It also has the capability to support counter-drug operations and consequence management, such as would occur after a terrorist event employing a weapon of mass destruction.[3]

USNORTHCOM will only provide military assistance to civil authorities when directed by the President or Secretary of Defense. Moreover, such assistance will always be in support of a lead federal agency, such as the Federal Bureau of Investigation or the Department of Homeland Security.[4]

The Federal Response Plan (FRP) determines which federal agency takes the lead in a specific incident. The type of incident determines the appropriate lead federal agency. According to the Federal Response Plan, there are two types of incidents: crisis management and consequence management. Crisis management is defined as "measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism…. Crisis management is predominantly a law enforcement response."[5] The lead federal agency for crisis management is the Department of Justice who delegates responsibility for crisis management to the Federal Bureau of Investigation.

Conversely, consequence management is defined as, "measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism."[6] State and local governments exercise primary authority to respond to the consequences of terrorism; the Federal Government provides assistance as required. In the case of a

consequence management scenario, the Department of Homeland Security would be the lead federal agency.[7] The figure below shows the overlapping nature of crisis management and consequence management.

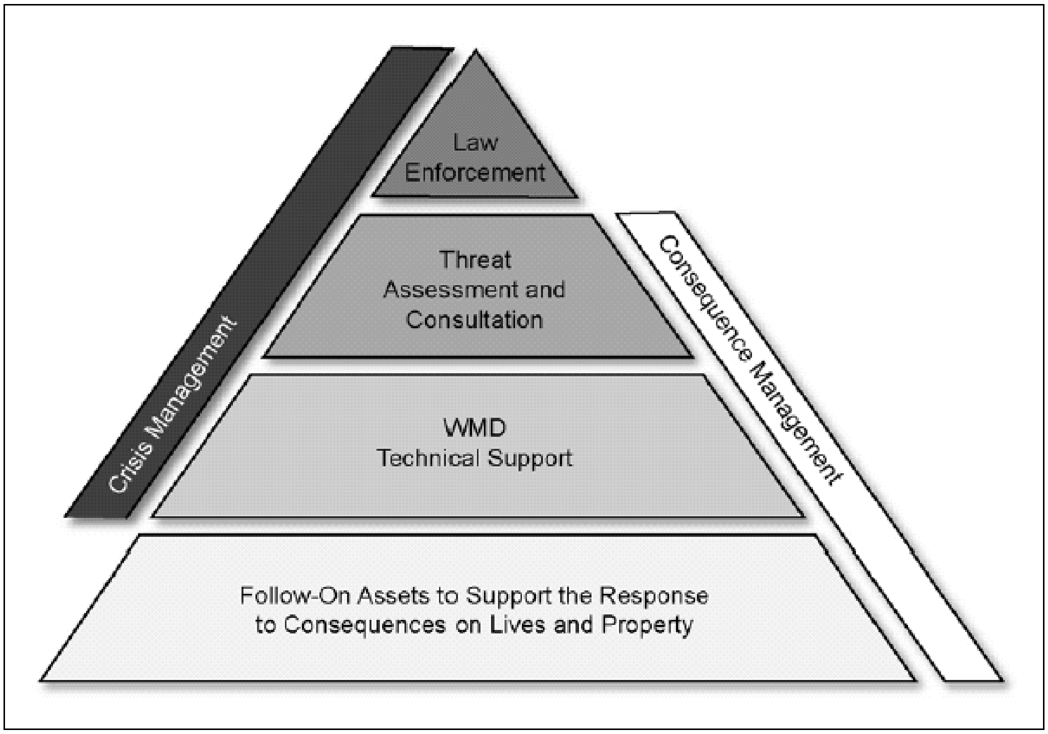

Figure 11. Relationship Between Crisis Management and Consequence Management[8]

State and local first responders are the first on the scene for most disasters and emergencies. If the situation exceeds the capability of the local and State first responders, the State may call on the federal government to provide additional assistance.[9] In situations that require military assistance, the requests would be relayed to the Department of Defense. Then, upon Secretary of Defense or Presidential direction, USNORTHCOM would respond with the appropriate forces and capabilities in support of the lead federal agency. When deploying forces in support of another lead federal agency, USNORTHCOM uses its Joint Task Forces (JTFs). Under its Joint Force Headquarters, USNORTHCOM currently has two standing JTFs: JTF-6 (Counter Drug)

and JTF-CS (Civil Support for WMD incident). If the situation dictates, USNORTHCOM could quickly standup additional JTFs tailored to the specific incident. The forces to populate those JTFs would come from other commands worldwide. Just as CENTCOM acquired forces from other commands worldwide to execute Operation Iraqi Freedom, USNORTHCOM can also draw upon forces provided by other commands. For example, if USNORTHCOM required Army forces to respond to an incident within the US, they could come from Army Forces Command. The forces would be assigned to the operational control of the JTF commander for that incident. The Federal Response Plan describes the DoD response as follows:

> Based on the magnitude and type of disaster and the anticipated level of resource involvement, DoD may establish a Joint Task Force (JTF) or Response Task Force (RTF) to consolidate and manage supporting operational military activities. Both task forces are temporary, multi-service organizations created to provide a consequence management response to a major natural or manmade disaster or emergency. The JTF responds to major disasters such as hurricanes or floods. The RTF responds to events involving the use, or possible use, of chemical, biological, and/or highly explosive agents/materials.[10]

Because of the coordination and assessment process for civil support, USNORTHCOM refers to itself as the "Heavy Lifter of Last Resort." Moreover, they see themselves as "the last to arrive, the first to leave, and will always respond in support of the lead federal agency."[11] The figure below illustrates the chain of events that would eventually result in the deployment of forces under USNORTHCOM's command.

Figure 12. USNORTHCOM's Role in the Federal Response Plan[12]

Changing from "Need to Know" to "Need to Share"[13]

One of the more pressing challenges facing USNORTHCOM is the need to share information both within DoD and with myriad national, regional, and local organizations that play a role in securing the homeland. In a consequence management scenario, USNORTHCOM truly serves as the "translator" organization between the military departments and civilian agencies. As the command responsible for Homeland Defense, it routinely operates within the DoD information context and approaches command and control from a traditional military perspective with clear chains of command and authority. As a result, its information architecture must enable traditional military command and control functions. At the same time, its information architecture must enable bi-directional flow of information with civilian agencies.

Over the past several years, DoD has put significant effort into maturing the communications functional area. Network Centric Warfare and the Global Information Grid have become foundational to military operations. Moreover, DoD has invested significantly in physical and human capabilities to innovate and improve the tools available to the information age warrior. These improvements aim to bring about decision superiority—to equip warriors and leaders with the right information, at the right time to make the right decisions.[14] Ideally, decision superiority will give US forces the ability to adapt more quickly in wartime and make it more difficult for an adversary to counter US military dominance. USNORTHCOM's information architecture must enable the military-to-military information flow while at the same time provide conduits for information flow to and from civilian agencies.

From an information architecture perspective, civil command and control systems have evolved from the local level with very little top-down direction and standards to enable "jointness." Major General Dale Myerrose, USNORTHCOM Director of Architectures and Integration, clearly identified this challenge of linking national-level organizations with states and other jurisdictions when he said that USNORTHCOM "provides an organization at the national level which links what we do in the Department of Defense with other departments and, hopefully, down to the states and other jurisdictions." [15] This recognition drives USNORTHCOM's information architecture efforts. As Gen Myerrose said, "I need to change my foundation from 'need to know' to 'need to share'" without compromising the security of sensitive information that could help an enemy."[16]

Information Sharing and P2P

One of the most significant efforts to share information in both crisis and consequence management scenarios is being championed by NORTHCOM. Through its Homeland Security/Homeland Defense Command and Control Advanced Concept Technology Demonstration Program (HLS/HLD C2 ACTD), USNORTHCOM is working to provide a tool for use throughout the entire homeland security establishment. The ACTD provides funding and program management for the Area Security Operational Command and Control System (ASOCC). This system incorporates client-server and P2P technology to "support the management of complex operations within an organization and among multiple agencies."[17] Moreover, "it has been shown to support DoD internal management requirements and coordination with and among other federal, state and local agencies and host nations."[18] ASOCC incorporates many tools such as the Defense Collaborative Tool Suite (DCTS), NetMeeting, chat and file sharing. It requires Windows 2000 and access to the Internet.

Like any capability provided on the commercial market, the true test of the system is whether people use it or not. That explains Microsoft's current dominance in the software market – people use their software. As USNORTHCOM continues to develop the ACTD into a more user-friendly system, the number of users will increase, the sharing of information through the ACTD in non-crisis situations will increase, and the system will become even more critical during times of crisis.

However, smaller jurisdictions, with limited budget capability will not be able to afford the significant investment required to acquire ACTD technology.[19] As a result, USNORTHCOM or another federal agency will need to consider how to allow

information sharing without the purchase of the ACTD standalone system. This is where P2P technology could play a significant role. By allowing users to access and share information through simpler and cheaper devices, even the edges of the network will be able to benefit from the wealth of information and interconnection that the ACTD brings.

As the heavy lifter of last resort, USNORTHCOM continually hones its skills and processes to ensure that it is ready whenever called upon. While serving at the nexus between military and civil authority, it will continue to adopt and adapt military and civil technologies to maintain its readiness to respond. As USNORTHCOM matures its information architecture, P2P technology will continue to provide a significant capability to enable information sharing across the entire homeland security domain.

Notes

[1] The military has been called to assist other federal agencies in disasters such as: Hurricane Andrew in Florida, Airport Security immediately after 9-11, Shuttle Columbia breakup (Feb 03), and forest fires in California.

[2] US Northern Command, "Who We Are – Mission," n.p., on-line, Internet, 6 February 2004, available from: http://www.USNORTHCOM.mil/index.cfm?fuseaction=s.who_mission.

[3] US Northern Command, "First Responders – The Role of USNORTHCOM," n.p., on-line, 6 February 2004, available from: http://www.USNORTHCOM.mil/index.cfm?fuseaction=s.first_role.

[4] US Northern Command, First Responders – The Role of USNORTHCOM, Available from: http://www.USNORTHCOM.mil/index.cfm?fuseaction=s.first_role

[5] Federal Emergency Management Agency, "Federal Response Plan – Interim," January 2003, TI-1, on-line, Internet, available from http://www.fema.gov/pdf/rrr/frp/frp2003.pdf.

[6] Ibid.

[7] Ibid., TI-3.

[8] Ibid., TI-2.

[9] Ibid., 11.

[10] Ibid., 15-16

[11] US Northern Command, "First Responders – The Role of USNORTHCOM," , n.p., online, Internet, 27 February 2004, available from:http://www.USNORTHCOM.mil/index.cfm?fuseaction=s.first_role.

[12] US Northern Command, "USNORTHCOM: Transforming the Defense of America." Briefing, 11.

Notes

[13] Master Sgt. Bob Haskell, "New Security Department Reinforces NORTHCOM Mission," *American Forces Information Service News Articles*, n.p., on-line, Internet, available from http://www.defenselink.mil/news/Nov2002/n11262002_200211262.html.

[14] Department of Defense, *Joint Vision 2020*, (Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000), 8.

[15] Haskell.

[16] Ibid.

[17] US Northern Command, "ASOCC Fact Sheet," 1.

[18] Ibid.

[19] Current cost of ASOCC terminal hardware and software is approximately $38,000. (Source: USNORTHCOM/J6, 14 Jan 04)

Chapter 5

Internationalizing Peer-to-Peer: North America and the World

> *My intuition is that we need to take NORAD to the next level… The types of disasters - man-made or natural - that we're talking about don't recognize borders.*
>
> General Ralph Eberhart,
> Commander, NORAD and USNORTHCOM

> *There is an important international dynamic, and Canada reflects this reality. It intensifies the relationship between the United States and Canada in respect to border security.*
>
> Paul Kennedy
> Canadian Senior Assistant Deputy Solicitor General

Although P2P technology may enable data sharing and communications for America's terrorism, criminal and disaster response needs, there will still be a geographical "edge" to this system. Just like the regional systems that are currently evolving, this edge will likely butt up against a non-compatible and non-sharing system. Thus, all the aforementioned interoperability problems will still exist. However, such problems will be compounded because they will occur at the American border where terrorists already know they can take advantage of the bi-national or multi-national agreements on border control, policing, citizen privacy rights, and the lack of interoperability for data and communications systems. Therefore, it is imperative that America works closely with its allies and neighbors in a collaborative manner to keep the communications flow open.

Peering Over the Border

Arguably, Canada is America's most important ally in the War on Terrorism. The two nations share the largest undefended border on the planet and they are co-dependent on bilateral trade. Over seventy-five percent of Canadian imports come from America while the United States has 17 states whose economies are dependent on Canadian trade.[1] Additionally, North American geography dictates that both nations are strategically interlinked with the defense of the other, hence the longstanding commitment of both nations to the North American Aerospace Defense Agreement (NORAD). Although the end of the Cold War brought changes to this relationship, militarily coordination is still needed. The recent shift in emphasis towards the War on Terrorism shows there is now more coordination required between the civilian agencies of these two nations. Fortunately, there is a long historical precedence for such cooperation.

A History of Collaboration

Since the World War II (WWII), the Canadian and US militaries have worked together extensively on interoperability. From the perspective of both nations, this made good sense. During the war, both were close allies and functioned almost as one entity on several North American military operations such as convoy duties, coastal patrol, secret agent training and some flight training.[2] After the war, the United States had not only superceded Canada's traditional military partner, Great Britain, as a dominant world power, but this occurred while Canada was exerting her independence as an equal among nations in contrast to its former "subject" role under Great Britain. Although equality is always subjective, military might is one measurement, and throughout the 1950's-60's, Canada would boast one of the top five militaries in the world, partly because of its

bilateral alliance with the United States, and partly because of both nations' roles in the new North Atlantic Treaty Organization (NATO). Finally, the strategic posture of the Cold War, combined with North American geography, demanded that these two nations cooperate and share military hardware and procedures.

In the communications arena, this cooperation began during WWII with the formation of the Combined Communications Board (CCB). Formed in 1941 between the US and UK, it included Australia, New Zealand and Canada as Commonwealth partners. In 1951, Canada became the first of the "junior" partners to become a full member, and since 1971, this board has been known as the Combined Communications-Electronics Board (CCEB) with headquarters in Washington D.C.[3] All military electronic and communications interoperability issues for the member nations are addressed through this forum.[4] It is interesting to note that Canadian military signals officers believe that the Canadian military services actually have better interoperability with their respective American service counterparts than jointly within the Canadian forces. This condition exists because most of Canadian military deployments and exercises were conducted as part of a coalition likely led, or at least headquartered, by the Americans which fostered a reliance on US communications procedures and technology.

For example, it appears that Canadian Army troops have better interoperability with American Army troops than with the Canadian Navy or Air Force.[5] This is interesting because, when compared to the civilian context, similar parallels can be found; it is in the civilian context that interoperability must occur. One premise of this paper asserts that the War on Terrorism blurs military and civilian functions and that, during a terrorist attack, civilian first responders essentially fill a military role. Therefore, traditional

military technology must now transfer to civilian agencies. Just as Canadian and American military forces have become interoperable, so too must both nations' first responders, especially law enforcement and border control agents.

Canadian Civilian Interoperability

First, although Canadian civilian organizations, especially first responder types, have developed their own unique communications and data sharing systems, these systems, like their Canadian military equivalents, tend to mirror their counterparts in the US. Some notable programs include the Canadian police emergency service "9-1-1" which operates exactly like its American sister system and the "Amber Alert" system, which rapidly notifies all police agencies and local communities if a minor is the victim of a suspected abduction. Another Canadian program is the Canadian Police Information Centre (CPIC) that operates in a similar manner to the American National Criminal Information Center (NCIC). The CPIC,

> Was created in 1966 to provide tools to assist the police community in combating crime… as a computerized information system to provide all Canadian law enforcement agencies with information on crimes and criminals. CPIC is operated by the RCMP under the stewardship of National Police Services, on behalf of the Canadian law enforcement community.[6]

Second, for those Canadian organizations, such as the RCMP, customs and border control, which regularly deal with their American counterparts, there is already a high degree of "interoperability."[7] In fact, when Lt Col Richert, the National Defense Fellow stationed in Canada, went to have an RCMP criminal background check conducted for the purposes of coaching youth basketball, the RCMP ran that check through the FBI. Both agencies already have co-use of each other's systems for these types of routine checks.[8] Once one thinks about this commonality, it probably appears somewhat

intuitive and expected from two nations that share so much technology, procedures and equipment, not to mention a common language. More interesting are the common pitfalls that have befallen the Canadians and how closely they mirror the American experience.

Just as the Americans had incidents that highlighted the vulnerabilities of their communications and data sharing architecture, so have the Canadians. Probably the most widely known Canadian incident resulted in the Campbell Commission where an independent commission reviewed the aftermath of multiple rapes in the Greater Toronto Area (GTA) that turned out to be the workings of a single serial rapist. The Commission found that several police jurisdictions had separate, sufficient amounts of information about various rapes that if put together would have led to the conclusion that this was all the work of a serial rapist and the probable capture of the suspect. However, these police agencies did not share their data and the rapes continued across jurisdictional lines for some time. As a result of the Commission's report, police jurisdictions in Ontario were cut from over 100 agencies to the current 42 and incorporated into the Integrated Justice Project (IJP). The IJP was instituted,

> As a joint initiative of the Ministry of the Attorney General and what is now the Ministry of Public Safety and Security (Ministries). The objective of the Project was to improve the information flow in the Justice system by streamlining existing processes and replacing older computer systems and paper-based information exchanges with new, compatible systems and technologies. In addition, a Common Inquiry System was to be created to allow authorized persons in one justice area to access and thus link to files held in other areas on cases, victims, witnesses, suspects, the accused, and convicted offenders. The Project was to affect approximately 22,000 employees in the Ministries at 825 different locations across Ontario, as well as municipal police forces, judges, private lawyers, and the general public.[9]

Additionally, these agencies are now becoming interlinked through the Ontario Police Tactical Information Centre (OPTIC) rather than relying on their antiquated and

"stove piped" data collection and dissemination systems. OPTIC is similar in architecture to regional American law enforcement communication and data sharing programs.[10] Although this consolidation streamlined the information flow for Ontario police agencies, cultural problems still existed. Just like American law enforcement agencies, the Canadians would have to break old barriers and forge new paradigms regarding access and the sharing of information. Therefore, if a system like JRIES were expanded to include Canadian first responders, especially law enforcement and border control, even more cultural barriers would have to be addressed.

Issues pertaining to individual privacy, law enforcement disclosure,[11] degrees of access to information by foreign nationals, and others, would require negotiation before implementation of any such system. Fortunately, these types of negotiations have been going on for years between these two nations, for example, they just recently began working on a plan for America to receive information about US bound airline passengers from Canada. This passenger information-sharing program is already under a pilot test program with European initiated flights.[12]

Peering Around the World

In cyberspace, borders are virtually irrelevant. Most commercially deployed P2P networks operate worldwide. With minimal effort and cost, P2P homeland security networks can easily expand to incorporate appropriate authorities in any country. Could JRIES even be expanded to Europe? Certainly some form of it could be, especially when one considers the military interoperability that already exists in NATO. Similar to the English speaking CCEB, NATO has the Multinational Interoperability Council that provides,

> A multinational forum for identifying interoperability issues and articulating actions, which if nationally implemented, would contribute to more effective coalition operations. It serves as the senior coordinating body for the member nations to resolve "information interoperability" issues and is intended to promote a responsive dialogue between key elements working coalition interoperability issues: defense policy analysts, operational planners, and C4I experts. The overall goal of the MIC process is to provide for the exchange of relevant information across national boundaries in support of the warfighter in coalition operations.[13]

Once again, these nations need to transfer this military interoperability to their respective civilian first responder agencies especially in the fields of law enforcement and intelligence. INTERPOL, the international police agency, is already a perfect forum to expand this type of information sharing across borders. Expanding INTERPOL's communications and data sharing architecture would open up a completely new realm of possibilities in tracking and investigating these new transnational threats. Moreover, INTERPOL, like NATO, already has years of experience handling language diversity. These two organizations seem ready-tailored to leverage existing military technologies, including P2P, to enable information sharing across international boundaries.

Peering Closer to Home

This difference in language highlights America's other neighbor, Mexico. Here too, expansion of JRIES or another P2P data sharing system seems not only practical; it seems doable. Similar to the Canadian/American experience, for many years these two nations have cooperated on immigration and drug trafficking programs. Therefore, transitioning, or expanding, to an anti-terrorism joint venture merely means hitch hiking on traditional cooperative agreements and systems already in place.[14] If adding Mexico makes sense, then adding the Caribbean and Central/South America seems like a natural transition, especially considering the growing connections between the international drug trade and

terrorism. Both crimes are transnational by nature; therefore, combating them requires a transnational approach as well. The process of expanding the communications and data sharing architecture of those agencies will enable all agencies to do a better job of combating these crimes. While cultural barriers will inhibit the acceptance of these technologies, the potential benefits far outweigh the costs. In a world where terrorists have equal access to rapid communications, travel and business, the systems in place to prevent, investigate and respond to acts of terror or other consequences must be the best they can be to combat any threat or attack. Therefore, America should continue to look to expand its communications and data sharing architecture with North, South and Central American neighbors, Europe, and ultimately the World.

Notes

[1] "Statistic Canada," Department of Foreign Affairs and Trade: Trade and Economic Analysis Division (EET) May 14, 2003, available from www.dfait-maeci.gc.ca/eet/.

[2] Interview with Lt. Col. John Anderson, Royal Canadian Air Force, Commander, 426 squadron, Trenton, Ontario, 10 Feb, 04; and, Lynn Phillip Hodgson, "Inside Camp X, the Top Secret WW II Secret Agent Training School," Blake Book distribution, Port Perry, Ontario, Canada, 2002; and, Commander Walter Karig, USNR, "Battle Report: The Atlantic War," Farrar & Rinehardt, Inc. New York, 1946, pp. 1-160.

[3] "An Introduction to the CCEB," on the Combined Communications and Electronics Board website, n.p., on-line, Internet, 20 January, 2004, available from http://www.dtic.mil/jcs/j6/cceb.

[4] Ibid.

[5] Interviews with Brig. Gen. (ret) William S. Richard, 36 year career Signals officer and former J-6 (Signals) for the Canadian Forces, Queen's University, Center for International Relations, Kingston, Ontario, 20 Jan 04; and, Major Jon Turner, British exchange officer commanding the Canadian Electronics and Communications Training Squadron, Canadian Forces Base, Kingston, Ontario, 22 Jan 04.

[6] Canadian Police Information Centre website, n.p., on-line, Internet, 20 January 2004, available from http://www.cpic-cipc.ca/English/index.cfm

[7] Interviews with various members of the Canadian Privy Council Office (PCO) and the Canadian National Defense Headquarters (NDHQ), Ottawa. Ontario, 11 Dec 03.

[8] Lt Col Richert's experience while stationed in Canada and conducting research for this paper.

[9] Ministries of the Attorney General and Public Safety and Security 4.03–Integrated Justice Project (Follow-up to VFM Section 3.03, 2001 Annual Report), n.p., on-line,

Notes

Internet, 20 January 2004, available from http://www.auditor.on.ca/english/reports/en03/403en03.pdf

[10] Interview with Inspector Merle Foster and Sergeant Roy Kendall (Technical support) of the Belleville Police Service, Ontario, Canada, 28 Jan, 04.

[11] Typically any communication medium such as voice or video that is used by the police becomes "disclosure" material in any subsequent investigation or trail. Therefore, cross-jurisdictional/border information and video could possibly become subpoenaed and these types of situations would have to be addressed.

[12] Jeremy Torobin, "Canada Might Give Airline Passenger Flight Data to the US," CQ Homeland Security News, n.p., on-line, Internet, January 30, 2004, available from, http://homeland.cq.com/hs/.

[13] Charter of the Multinational Interoperability Council, 2nd Edition, April 17, 2002, p. 2, n.p., on-line, Internet, 20 January 2004, available from http://www.defenselink.mil/nii/org/c3is/ccbm/mic.html.

[14] Discussions with Special Agent Perla Garcia-Alcocer with the Mexican Instituto Nacional Para el Combate a las Drogas while attending the FBI National Academy, 186th Session, 1996.

Chapter 6

Conclusion and Recommendations

Share by rule, withhold by exception.

Maureen Baginski, FBI Director of Intelligence, quoted at the
Government Convention on Emerging Technologies, Las Vegas, Nevada

The Homeland is more secure when each hometown is more secure.

Tom Ridge
Secretary of Homeland Security

Peering Into the Future

Peer-to-Peer (P2P) technology is about empowerment. It is about expanding situational awareness at the edges of the network and creating decision superiority across the entire crisis management and consequence management spectrum. More specifically, it offers first responders direct access to each other, to time-critical information, to sensors, and, ultimately, to unprecedented knowledge of the incident at hand, which facilitates the rescue of people and minimizes damage. Moreover, before an incident, it offers investigators the ability to get inside the decision cycle of an adversary and possibly prevent a terrorist attack before it even begins.

As this paper illustrates, P2P technology can improve current Homeland Security crisis-response elements and benefit first responders and their respective agencies.

Moreover, it shows how USNORTHCOM can leverage P2P technology to facilitate DoD's role in consequence management. It offers a tremendous opportunity to bring greater situational awareness and enhance the ability of first responders to coordinate actions at the scene of an incident. However, like any new technology, P2P brings with it promises and perils, strengths, and vulnerabilities (See Appendix D). The difficulty lies in the balance between risk and reward. One extreme would be to pursue the promises and ignore the perils while the other extreme would be to focus only on the perils and miss the promises.

Is the reward worth the risk? This brings one back to the challenges confronting strategic decision makers today—peacetime uncertainty. In the case of P2P technology, the true risk and reward is unknown today. Ultimately, the only way to completely answer that question is to experiment and try it—put P2P technology through its paces and see if it can live up to its promise and improve battlespace (crisis/consequence management) awareness.

However, technology is only one small part of the changes necessary to bring about improved communications and situational awareness. For example, the military continues its efforts to bring decision superiority so that US forces are far ahead of any adversary. A US Joint Forces Command proposal for a Common Relevant Operating Picture states, "the success of future data collection and processing, information dissemination, and knowledge presentation depends on having the *right* people, in the *right* place, at the *right* time to ensure the application of this technology. Technology, by itself, is not the master of our future."[1] Considering that the battlefield of today could be anywhere, this also applies to the civilian arena. If another major terrorist attack were to

be attempted upon America, getting the right people, in the right place, at the right time will be critical to preventing it or mitigating the results. As this paper has shown, P2P technology facilitates this process immensely. However, there is still the major challenge to this process, namely, culture.

It's About Culture

Zoë Baird and James Barksdale from the Markle Foundation's Task Force on National Security in the Information Age state,

> The biggest obstacle to implementing the best designed systems in the world is often culture. Organizations, processes, and technologies can be changed, but unless fundamental changes occur in the culture of the participants in an existing system, progress is stymied.[2]

Essentially, it comes down to changing people and their standard operating procedures--their habits of relating. Peter Roy, Chief Technology Officer for the Washington D.C. Metropolitan Police Department puts it this way, "Technology is the *easy* part. Business process is the *hard* part… we can create pipes to connect anyone, the real question is, will they use it?"[3] Thus, it is not only technology that limits effectiveness, but culture as well. P2P technology, if adopted, will require cultural, organizational, doctrinal, and other changes to be effective.

The information revolution continues to drive change in the business community, in government, in the military, and for first responders. Although this technical revolution is moderated by many factors such as culture, strategy, policy, organization, doctrine, fiscal constraints, and strategic environment, culture remains the most significant factor. Moreover, it takes more time for culture change than technological change. As Retired

Vice Admiral Tuttle postulated in a presentation to the Joint Military Intelligence College,

> When a new age is entered, technology leads by two decades the organizational, policy, strategy, doctrinal, operational procedures and cultural changes necessary to exploit the technologies. The limiting factor in progress is not our ability to imagine the future or invent it, but our willingness to embrace it.[4]

Therefore, organizations should expect that there would be a "learning curve," or period of time to adapt to using P2P technology. What they are likely to find is that, instead of problems with P2P technology, users will explore and exploit new ways of using it that were previously unimagined.

Recommendations

The first major recommendation is for the DHS to establish a nationwide P2P system. As already noted in Chapter 2, one system, JRIES, was launched in September 2001 and in late February, 2004, DHS "announced the expansion of its computer-based counterterrorism communications system to all 50 states, five territories, Washington, D.C., and 50 major urban areas."[5] However, this P2P system is specific to the War on Terrorism and law enforcement focused. Furthermore, even though NORTHCOM is connected to this system, it is still P2P in its infancy. This system, or a system like it, should be expanded to all civilian first responders and crisis management agencies to allow a more synergistic effort. Of note, Tom Ridge, Secretary of DHS announced on 23 February 2004 that, "The Department has identified technical specifications for a baseline interoperable communication system," that, "If adopted at the state and local level, by the end of 2004, most first responders will have a way to communicate with each other

during a crisis, regardless of frequency or mode of communication."[6] This is the ultimate goal and should be pursued to the fullest.

Second, although the benefits of P2P technology are clear, little study has been done to illuminate the cultural and procedural challenges that would result from the deployment of such a system for first responders. A true P2P system would allow direct connection between first responders from myriad agencies such as local police, fire, emergency medical technicians, to the FBI, DHS, NORTHCOM and countless other agencies at all levels of government. Each user or agency has its own unique culture and standard operating procedures that shape its actions and operations. Thus, it would be beneficial to study ways to mitigate the negative effects of culture clashes that will inevitably occur while deploying a P2P capability.

Third, NORTHCOM should fully integrate military response forces (JTFs and RTFs) into training and exercising with their civilian counterparts so they are interoperable before a terrorist or disaster occurs. At a minimum, this would entail linking various military organizations such as National Guard units, military police and chemical weapons response forces, to the JRIES system and to the new DHS communications architecture.

Fourth, the DoD and the USAF, (specifically the National Defense Fellows and Force Protection Battle Lab programs), should take advantage of both the DHS Homeland Security Center of Excellence, established at the University of Southern California, and, the DHS Fellows program where over one hundred fellows are "dedicated to pursuing new technologies to protect the homeland."[7]

Finally, the United States should continue to expand interoperability relationships with other nations and international organizations to foster increased information exchange and database access. In this case, more information is always better than less information.

Future Research

As P2P technology in the commercial context becomes more commonplace and takes its position with the client-server model in the information domain, the Department of Homeland Security is taking steps today to understand and leverage the capabilities that P2P technology brings.

Although the technology is still immature, and various corporations are competing to produce an infrastructure to support P2P applications, it is never too early to begin thinking about the potential of this new technology. Some initial steps would include: 1) conduct an in-depth analysis and review of P2P possibilities for first responders, 2) experiment with P2P concepts and applications in a Homeland Security training environment, and 3) train software developers and first responder personnel on P2P applications and their possibilities. Another fruitful area of research would be to consider how to counter an adversary that might deploy a P2P system.

In conclusion, P2P technology is about enabling people. It does this by enabling information-rich interaction at the edges of a network and between the most intelligent parts of any network—the people. Only people can uniquely adapt to changes in the operating environment and P2P technology gives them the right information at the right time to make the right decisions.

Notes

[1] US Joint Forces Command Concepts Division, "A White Paper for The Common Relevant Operating Picture," (Draft White Paper, version 1.1, Norfolk, Virgina, 21 April 2000), 1-0.

[2] Zoë Baird and James Barksdale, "Creating a Trusted Network for Homeland Security," Markle Foundation, Task Force on National Security in the Information Age, 22, n.p., on-line, Internet, 26 February 04, available from http://www.markletaskforce.org/Report2_Full_Report.pdf.

[3] Peter Roy and Joe Ross, Office of the Chief of Technology, D.C. Metropolitan Police Department, interview with authors, Washington D.C., 4 December 2003.

[4] Jerry O. Tuttle, "Decision Superiority and Intelligence," Defense Intelligence Journal, September 2000, 70.

[5] US Department of Homeland Security, "Homeland Security Launches Expansion of Information Exchange System to States and Major Cities," Official Press Release, n.p., on-line, Internet, February 24, 2004, available from http://www.dhs.gov.

[6] Alice Lipowicz, "Ridge Proposes Plan to Link First Responder Radios," Congressional Quarterly, Homeland Security – Local Response, n.p., on-line, Internet, 20 February, 23, 2004, available from http//www.cq.com.

[7] US Department of Homeland Security, "New Homeland Security Scholars and Fellows Accept Awards," n.p., on-line, Internet, Septemberber 23, 2003, available from http://www.dhs.gov/dhspublic/display?theme=43&content=1716.

Appendix A

Notional Vignette

All ideas and thoughts in the following notional vignette are solely those of the authors and are imaginary. In reality, all of the agencies described below are truly playing significant roles in developing solutions to the problems highlighted in the vignette below.

The following summary is taken from a notional TOP SECRET British Foreign Intelligence (MI-6) report regarding the events leading up to and surrounding the terrorist attacks against the United States that occurred on July 4th 200x.

MI-6 Foreign Intelligence Summary:

This summary gives a snapshot account of the attacks and some details are based on partial analytical conjecture; however, in addition to receiving the American and Canadian reports, several suspected members of the terrorist plot were detained post-incident in the United Kingdom and were interrogated by MI-6.

On July 4th 200x, two nearly simultaneous pre-coordinated terrorist attacks, attributed to an offshoot group connected to Al Qaida, were launched against the United States, specifically targeting the ports of Newark, New Jersey, and Long Beach, California. The intended impact of these attacks was well thought out. Close to 60% of the over nine million ship containers that enter the United States annually, pass through

these two ports. Shutting them down would be devastating to the North American and world economies.[1] Additionally, the attack planning appears to have gone on in secrecy for some time and the attacks were intended to be covert. Despite this, the attack on Long Beach achieved only limited success and the Newark attack was completely thwarted before it began. This was mainly due to pre-attack investigative interoperability and coordination (for Newark) and post attack response interoperability/coordination (for Long Beach). In both instances, an emerging technology known as Peer-to-Peer (P2P) enabled unprecedented situational awareness that allowed investigators and first responders to dominate the decision cycle and disrupt the terrorist's intentions. Unfortunately, the West Coast P2P program was not as mature as its corresponding East Coast counterpart, which accounts for the partial success of the terrorist plans at Long Beach.

Those plans entailed the use of hijacked container ships as the means of delivering the terrorists and their explosives to their targets. In both cases, the terrorists intended to ram their targets and then detonate various amounts of explosives mixed with hazardous cargo to create a sort of "dirty" bomb effect in the hopes of putting the ports out of commission for extended periods.

The Long Beach attack was launched from a terrorist cell operating out of Vancouver, British Columbia, whereas the Newark attack cell operated out of Montreal, Quebec. Although some of the terrorists were Arab, most appear to have Asian Pacific origins, mainly Indonesian and Philippino. All either had emigrated to Canada or were living and working there under student/worker visas for various numbers of years. The terrorists took jobs as dock workers and cruise boat hands and some even enrolled in

ship-handling courses. Both the East and West Coast cells trained on and conducted surveillance of their targets using large off-shore commercial fishing craft they purchased with funds generated through an illegal immigration ring they controlled (specifically bringing young Chinese and other Asian-Pacific women into Canada for massage/prostitution spas, sweat shops, and as domestic laborers). These fishing boats were subsequently used to hijack the large container ships off the coasts of America. Moreover, co-terrorists who had already landed jobs on them at their homeports of Singapore and Rotterdam assisted in the hijacking incidents. Both ships were then rigged up as "dirty bombs" with explosives placed in and around the hazardous portions of the cargos they were carrying.

The Long Beach bound ship, the *Kobe Maru*, carried liquid chlorine, whereas the Newark ship, the *Jobert Bouta*, carried anhydrous ammonia, a high-grade fertilizer, in pellet form. Both ships were guided to their respective ports arriving on schedule, but departed from normal procedures upon entering local shipping channels. Unfortunately, due to a lack of pre-attack investigative coordination, the Long Beach terrorists were able to ram the *Kobe Maru* into one of the major off loading piers/derricks and the subsequent explosion and hazardous cloud killed or wounded several hundred dockworkers and local residents. The harbor facilities are currently estimated to be operating at sixty percent of pre-attack capacity with an estimated eight to ten months required to gradually return to full operations. Despite the failure of pre-attack intelligence and other coordinating efforts to stop the Long Beach terrorists, the subsequent disaster response was well coordinated and significantly reduced the potential for further damage to life and

property. Critical to this response was the robust P2P information sharing system already established among Los Angeles-area first responders and disaster response forces.

On the other side of America, the second terrorist attack was completely thwarted. Most of the terrorists were captured, except for those who committed suicide or were killed during the assaults on their ships by authorities. The reason for this success is detailed extensively throughout the co-American/Canadian report of the incident. That report credits P2P data sharing and data mining-capability for "connecting the dots" and linking the many disparate pre-attack investigations into a coordinated effort that was able to preempt the Newark terrorist attack.

Even though the seeds of this success were planted prior to the "9-11" attacks, it was those attacks, where over 300 firefighters died due to communications interoperability failure, that highlighted just how poor the "first responder" (law enforcement, medical, fire department, civil disaster) interoperability situation was. Similar to the American military's "Desert One" incident in Iran in 1979, where dramatic mission failure subsequently alerted senior US officials to the need for compatible equipment for the armed services, 9-11 became the clarion call for first responders in a similar way. All across America, different emergency/disaster/terrorist response groups began focusing on increasing data flow across agencies and communities. Nowhere was this more emphasized than in the area surrounding Washington D.C. First, the D.C. Metro Police launched the "D.C. Mobile" program, inter-connecting all their vehicles with data and video capability. This was then incorporated into the greater Virginia and Maryland "CapWIN" program, which linked all first responders, plus various federal agencies (Federal Bureau of Investigation (FBI), Secret Service, Capitol Police, Departments of

Transportation, Department of Homeland Security, Federal Emergency Management Authority, Coast Guard, and others) into one cohesive data sharing system. Finally, in late 2003, the Department of Homeland Security (DHS) approved the Joint Regional Information Exchange System (JRIES), a P2P planning, data sharing and attack response program, as the nationwide terrorism threat analysis system. As for Canada, starting in 2004, under the leadership of the Paul Martin administration, Canadian agencies began closer cooperation with their American counterparts. One trial program added the Royal Canadian Mounted Police (RCMP), the Ontario Provincial Police (OPP), the Quebec Provincial Police, the Canadian Customs and Revenue Agency (CCRA), the Citizenship and Immigration Canada (CIC) and various other Canadian agencies into the JRIES data sharing system of the Americans. Unfortunately, this trial program was not extended to Canada's Western Provinces. The stage was thus set prior to the terrorist attacks of July 4.

On the East coast, the first agency to raise the alarm was the RCMP when several members of an illegal immigration ring that was under surveillance turned up on a US Coast Guard facial recognition inquiry run through JRIES. US Coast Guard intelligence experts had photographed the terrorists on several occasions as part of the new customs and border control procedures that dictated photographing all vessels penetrating a 150-mile zone of the American coast. After confirming the identities of the individuals, the RCMP sent an "alert" message back through JRIES and began tighter surveillance. These actions also began a coordinated series of investigations by multiple agencies (RCMP, FBI, Central Intelligence Agency (CIA), DHS, etc.) using JRIES as their communicative/data-sharing tool.

Just prior to the July 4th holiday period (July 1st is Canada Day), after the US once again increased its terrorist threat warning to Condition Orange, the RCMP began verifying the locations of these individuals. They discovered that most of them had departed their residences, had closed bank accounts and had finished other personal business. The RCMP immediately sent its counterparts throughout Canada and the United States another alert message that immediately brought pictures, intelligence dossiers and investigation background information to literally hundreds of agencies and individuals with access to JRIES. The Canadian Air Force located the fishing vessel and turned over tracking to the US Coast Guard after the boat entered international waters South of the St. Lawrence Seaway. During the night of July 3rd, the terrorists intercepted the *Jobert Bouta* approximately 120 miles off Long Island, New York and, with the help of their co-conspirators aboard, took control of the ship. By this time, the FBI, using JRIES, alerted the entire Eastern Seaboard. Simultaneously, the US military, along with several federal and local police agencies, planned a joint counter-strike operation. This assault occurred on the night of July 3rd when a US Navy SEAL team covertly boarded the large container ship while it met the Newark harbor pilot boat. On board the Pilot boat were several members of the New York City SWAT team who assisted in the ship's recapture. During this covert operation, the JRIES network handled all communications across agency lines.

Undercover Coast Guard and New York City Police apprehended the terrorist's fishing boat as it approached the Verrazano Narrows Bridge where the terrorists had planned to ram the bridge. The unsuspecting terrorists were captured en-mass. Again, communications between all agencies involved were handled through JRIES. Upon the

terrorists' capture, US Authorities contacted counterparts in Rotterdam and around the world who began further investigation, which is how MI-6 entered the investigation.

Unfortunately, all this was too late to prevent the attacks on the West Coast, where JRIES was operating, but only at the local level. Whereas the East Coast pre-incident investigation was (nationally and internationally) coordinated from the beginning, the West Coast suffered through a situation similar to that leading up to the September 11, 2001 attacks on America. On the West Coast, information overload, failure to communicate critical information in a timely fashion, and lack of coordination among investigators, contributed to a tragic chain of events. Although JRIES was championed by former Governor of California Arnold Schwarzenegger, the California legislature did not support internationalizing it with Canada and Mexico, as the expenditure was considered too great when compared to the immigrant health care crisis. Once California disapproved an international JRIES, the rest of the Western States could not continue the program alone and it remained a national/local network.

As for the Canadians, the RCMP in Vancouver had several of the terrorists from the illegal immigration ring under surveillance but did not interface with the Americans. Upon learning of the terrorists' disappearance, they only contacted up their local chain of command, as there was no West Coast American JRIES with which to network. This data made its way back to Ottawa, Canada, where the RCMP Headquarters contacted the State Department and FBI via JRIES. The FBI contacted the Border Protection and Customs agency and a BOLO (Be On the Look Out) report was generated, but unfortunately, contained no immediate pictures and the terrorists were already out to sea in their fishing vessel. Here too, the RCMP eventually realized the terrorists were at sea

but communication once again went through the old established chain of command and precious time was lost contacting the Americans. By the time the US Coast Guard was alerted, the terrorists had commandeered the *Kobe Maru* and sped South towards Long Beach while the remaining terrorists continued towards San Francisco in an attempt to ram the Golden Gate Bridge. The US Coast Guard stopped this boat, but the terrorists detonated explosives and killed all aboard. Meanwhile, as the *Kobe Maru* approached the California coastline, the story of the Newark attack's failure was leaked by an excited New York TV station that wanted to scoop the story. This was immediately picked up by CNN and broadcast globally. Since the West Coast terrorists now knew that their compatriots had failed, they changed tactics and no longer met up with the pilot boat and tugs that came to meet them at Long Beach. Pilot Boats and tugs, that now carried additional Coast Guard and local police, tried to check every ship and boat in harbors approaching the West Coast; an onerous task at best. Instead, the terrorists increased speed, exchanged gunfire with the few small Coast Guard vessels and police helicopters that attempted to stop them, and continued. Attempts to coordinate with local military ships and aircraft that could have stopped them was slowed by lack of communications interoperability and a decision making freeze, thus allowing enough time for the terrorists to ram into their target and blow up their ship.

Fortunately, the resulting emergency response teams were linked together and were as coordinated as their East Coast counterparts. The entire California disaster response network had been alerted through JRIES, and multiple agencies were already responding when the *Kobe Maru* exploded. Using P2P technology, the on scene commander tapped into a national network of HAZMAT specialists who immediately assisted local

responders to form ad hoc, cross functional teams even while en-route to the scene. Again, using P2P links, these teams communicated directly with such organizations as the Centers for Disease Control in Atlanta and the US Army's Chemical Weapons training site at Fort Leonard Wood, Missouri. These links provided critical information to first responders and follow-on recovery teams such as Federal Emergency Management Agency (FEMA) and National Guard forces. The links were also active to local hospitals as well. Taken together, this information exchange dramatically reduced the loss of life and property. In essence, P2P technology empowered all those responding by exponentially increasing situational awareness. Moreover, it linked those on the edge of the network who owned critical time-sensitive information directly with those who needed it.

One positive outcome of this tragedy is that the California legislature, in emergency session, approved an emergency budget expenditure to launch a West Coast internationalized JRIES network. These improvements aim to bring about decision superiority—to equip warriors and leaders with the right information at the right time to make the right decisions.[2] In today's environment, first responders are the warriors and leaders who need the right information at the right time to make the right decisions.

Notes

[1] Jayson P. Ahern, Assistant Commissioner, US Customs and Border Protection, Opening remarks to the E-Gov Conference on Homeland Security, Washington D.C., 2 Dec 2003. (The US maintains over 400 points of entry into the country. Of these, the ports of Long Beach and Newark are the most heavily used. In fact, the port of Long Beach is considered the world's largest port facility when compared by volume of containers annually transported accounting for over 43% of all the containers that enter America.).

[2] Department of Defense, *Joint Vision 2020*, (Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000), 8.

Appendix B

Key Homeland Security Stakeholders

> *We're fighting a new kind of war against determined enemies. And public servants long into the future will bear the responsibility to defend Americans against terror.*
>
> President George W. Bush

Since the attacks of 9-11, many homeland security organizations and businesses have been created, while many existing entities have been reengineered to better structure them for homeland security planning and response. This section will review some important conceptual distinctions and highlight the various homeland defense / security organizations and their associated roles and responsibilities.

Homeland Defense vs. Homeland Security

The distinctions between homeland security and homeland defense are central to understanding the roles and responsibilities of the myriad organizations involved in securing the homeland. Homeland defense is defined as:

> The *protection of United States* territory, domestic population, and critical defense infrastructure against *external threats and aggression*. It also includes routine, steady state activities designed to deter aggressors and to prepare US military forces for action if deterrence fails (emphasis in original).[1]

By contrast, homeland security is defined as:

> A concerted *national effort* to prevent *terrorist attacks* within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage and assist in the recovery from terrorist attacks. (emphasis in original).[2]

If there is an attack on the homeland, homeland defense and security overlap. The Department of Defense (DoD) has always been the lead agency responsible for homeland defense. DoD has always had military forces available to provide assistance to civil authorities and first responders. Nevertheless, these have always been deployed in support of another federal agency. Defined as Civil Support (CS), DoD maintains the capability for first responders and military forces to work together in response to an attack. DoD defines civil support as:

> DoD support to US civil authorities for domestic emergencies and for designated law enforcement and other activities. CS missions are undertaken by DoD when its involvement is appropriate and when a clear end state for the DoD role is defined.[3]

Planning is critical to ensure that DoD forces and capabilities are ready to support when called for by the President or the Secretary of Defense. DoD has defined Emergency Preparedness as:

> Those planning activities undertaken to ensure DoD processes, procedures and resources are in place to support the President and Secretary of Defense in a designated National Security Emergency.[4]

The figure below illustrates the overlapping nature of homeland defense, homeland security, civil support and emergency preparedness.

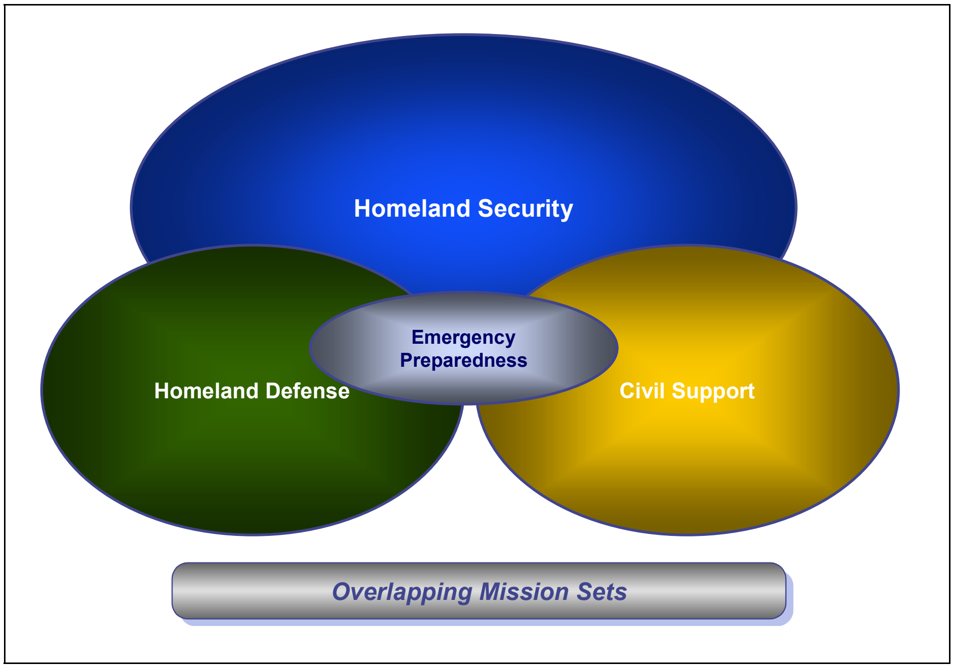

Figure 13. Homeland Security and Homeland Defense Paradigm[5]

Organizational Roles and Responsibilities

Many organizations play a role in securing the homeland. At the national level, the most significant organizations are the Department of Homeland Security (DHS), DoD, and the Department of Justice (DOJ). Each institution organizes itself to accomplish its primary missions. It is important to understand the missions and responsibilities of each of the major organizations. Later chapters will draw on this background material.

Department of Homeland Security (DHS)

Established in 2002, the Department of Homeland Security (DHS) is charged with the following responsibility.

> (A) prevent terrorist attacks within the United States;
> (B) reduce the vulnerability of the United States to terrorism; and
> (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.[6]

By March 2003, over 180,000 people from twenty-two agencies had been merged into its structure.[7] These agencies include the Secret Service, the Coast Guard, the Customs Service, the Federal Emergency Management Agency (FEMA), and many other organizations. It is currently organized with the following major bureaus: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Assurance and Infrastructure Protection.[8] The figure below illustrates its organizational structure.

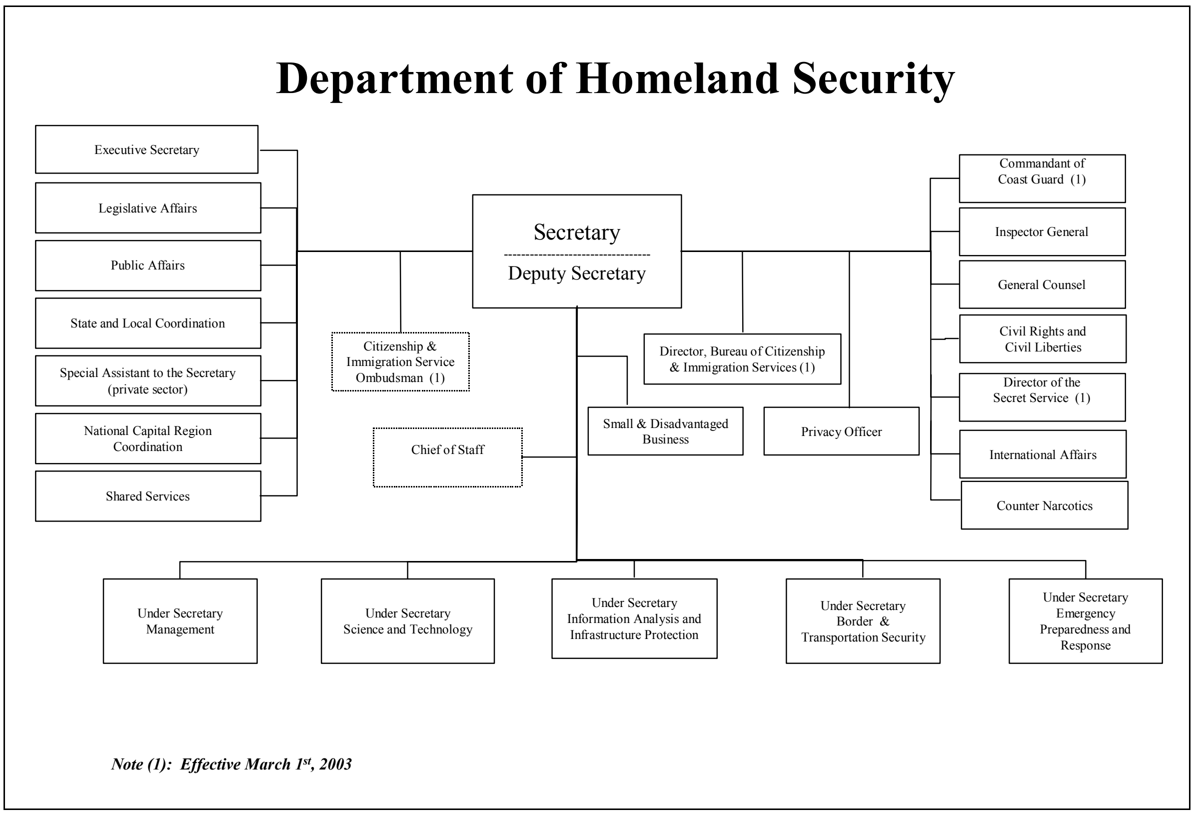

Figure 14. Department of Homeland Security Organizational Chart[9]

Department of Defense (DoD)

DoD's mission is to provide the military forces needed to deter war and to protect the security of the United States.[10] DoD is organized to accomplish its operational mission

worldwide through operational combatant commanders who respond to the direction of the President and the Secretary of Defense. The military is trained and equipped through the Services (Army, Navy, Air Force, and Marines). Over all of these organizations is the Office of the Secretary of Defense (OSD) that serves as the policy-making office to give policy direction to the Services, the Joint Staff and the combatant commands.

Authorized by Congress in the FY03 Defense Authorization Act, the Assistant Secretary of Defense for Homeland Defense **(ASD(HD))** is responsible for the "overall supervision of the homeland defense activities of the Department."[11] The honorable Paul McHale was appointed as the first ASD(HD) in March 2003 and given responsibility by the Deputy Secretary of Defense for "all DoD homeland defense activities, all DoD civil support and emergency preparedness activities, all DoD domestic crisis management activities, and to serve as the principal DoD interface with the new Department of Homeland Security."[12] The Office of the ASD/HD is organized as shown in the figure below.

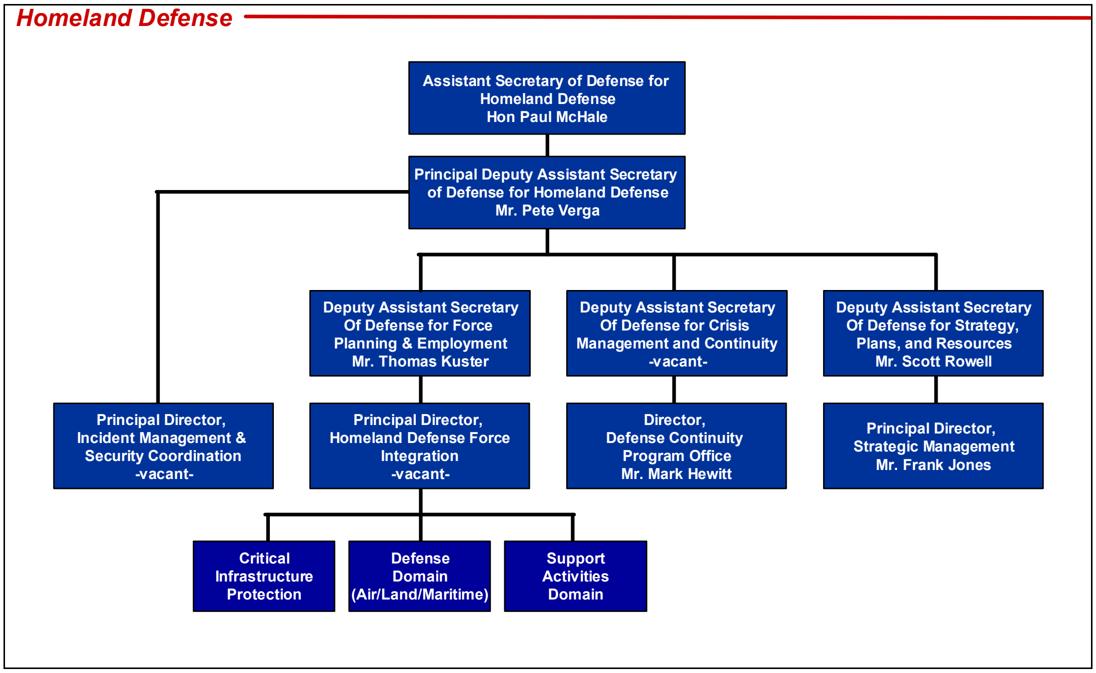

Figure 15. Office of the Assistant Secretary of Defense for Homeland Defense Organizational Chart [13]

The President or the Secretary of Defense, with the advice of the Chairman of the Joint Chiefs of Staff, exercises authority to deploy troops and exercise military power through nine unified commands.[14] Last updated in October 2002, the Unified Command Plan (UCP) outlines the areas of responsibility for each Combatant Commander. There are five regional commands and four commands with worldwide responsibility. The regional commands are shown in the figure below. Those commands with worldwide responsibility are: US Transportation Command, US Strategic Command, US Special Operations Command, and US Joint Forces Command.

Figure 16. Combatant Command Areas of Responsibility[15]

US Northern Command (USNORTHCOM)

US Northern Command (USNORTHCOM) is the combatant command responsible for homeland defense and providing military assistance to civil authorities. Its area of responsibility includes the United States, Canada, Mexico, parts of the Caribbean and the contiguous waters in the Atlantic and Pacific oceans up to 500 miles off the North American coastline. USNORTHCOM's mission is to:

> Conduct operations to deter, prevent and defeat threats and aggression aimed at the United States, its territories and interests within assigned areas of responsibility; and as directed by the President or Secretary of Defense, provide military assistance to civil authorities, including consequence management operations[16]

When directed by the President and Secretary of Defense, USNORTHCOM serves as the military headquarters to provide support to civilian agencies. It provides the military link between civil authorities and DoD forces. As a result, it must be able to communicate effectively both within and outside of DoD.

Department of Justice (DOJ)

The Department of Justice plays a significant role in preventing, investigating and prosecuting terrorist attacks. Moreover, it is responsible for crisis management, which is "measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism."[17] The Attorney General of the United States leads the Department of Justice in its mission as follows:

> To enforce the law and defend the interests of the United States according to the law; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; to administer and enforce the nation's immigration laws fairly and effectively; and to ensure fair and impartial administration of justice for all Americans.[18]

Federal Bureau of Investigation (FBI):

While DOJ serves as the lead federal agency for crisis management, it has delegated that responsibility to the FBI.[19] The mission of the FBI is to:

> To uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; to provide leadership and law enforcement assistance to federal, state, local, and international agencies; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States.[20]

With respect to Homeland Security, the FBI has responsibility for collecting intelligence to identify and counter the threat posted by terrorists. It also develops count-terrorism initiatives to minimize the threat that terrorists pose to Americans and the critical infrastructure of the country.[21]

First Responders

Every crisis or terrorist attack is local. It is the local first responders that will be first on the scene, first to take action, and first to take command of the scene. In most cases,

the local first responder leadership will be responsible to lead the entire response effort from beginning to end. First responders are "the men and women who are 'first on the scene' as a natural or man-made disaster unfolds, … also the last to leave the scene."[22] They are the over 11 million state and local individuals from over 87,000 jurisdictions that serve as police officers, firefighters, emergency medical technicians and others.[23] This research focuses on delivering the capability for first responders to achieve decision superiority—the right information, at the right time to make the right decisions.[24]

Notes

[1] Peter F. Verga, "Homeland Defense," Briefing at Government Convention of Emerging Technologies," 8 Jan 04, Las Vegas, 3.

[2] Ibid. Mr. Verga's briefing noted that these definitions were originally identified in DoD's Joint Operating Concept (JOC) for Homeland Security, tasked by the Joint Requirements Oversight Council, coordinated by NORTHCOM (Draft).

[3] Ibid., 9.

[4] Ibid.

[5] Ibid.

[6] Homeland Security Act of 2002, Public Law 107-296, 107th Cong., 25 November 2003, Sec 101 (b) (1) (C), on-line, Internet, 24 February 2004, available from http://www.cio.gov/documents/pl_107_296_nov_25_2003.pdf.

[7] "The US Department of Homeland Security: Preserving Our Freedoms, Protecting Our Nation," *Department of Homeland Security*, n.p., on-line, Internet, 24 February 2004, available from http://www.dhs.gov/dhspublic/display?theme=10&content=3206.

[8] "DHS has Five Major Divisions, or "Directorates":," *Department of Homeland Security*, n.p., on-line, Internet, 24 February 2004, available from http://www.dhs.gov/dhspublic/display?theme=9&content=2973.

[9] Department of Homeland Security, "Department of Homeland Security Organizational Chart," n.p., on-line, Internet, 24 February 2004, available from http://www.dhs.gov/ dhspublic/interweb/assetlibrary/DHS_Org_Chart.ppt.

[10] Department of Defense, "Our Bottom Line," 47, on-line, Internet, 26 February 2004, available from http://www.defenselink.mil/pubs/dod101/dod101for2002/ dod101for2002_files/frame.htm.

[11] National Defense Authorization Act for Fiscal Year 2003, Public Law 107-314, 107th Cong., 2 December 2002, Sec 901 (a) (3); on-line, Internet, 24 February 2004, available from http://www.defenselink.mil/dodgc/lrs/docs/ PL107-314.pdf.

[12] Peter F. Verga, "Homeland Defense," 5.

[13] Ibid., 7.

Notes

[14] Department of Defense, "Unified Commanders," 29, on-line, Internet, 26 February 2004, available from http://www.defenselink.mil/pubs/dod101/dod101for2002/dod101for2002_files/frame.htm.

[15] Department of Defense, "Unified Command Plan," n.p., on-line, Internet, 26 February 2004, available from http://www.defenselink.mil/specials/unifiedcommand/.

[16] US Northern Command, "Who We Are – Mission," n.p., on-line, Internet, 26 February 2004, available from http://www.northcom.mil/index.cfm?fuseaction=s.who_mission.

[17] Federal Emergency Management Agency, "Federal Response Plan – Interim," January 2003, TI-1, on-line, Internet, available from http://www.fema.gov/pdf/rrr/frp/frp2003.pdf.

[18] Department of Justice, "Overview," n.p., on-line, Internet, 27 February 2004, available from http://www.usdoj.gov/jmd/mps/manual/overview.htm.

[19] Federal Emergency Management Agency.

[20] Department of Justice, "Federal Bureau of Investigation," n.p., on-line, Internet, 27 February 2004, available from http://www.usdoj.gov/jmd/mps/manual/fbi.htm.

[21] Ibid.

[22] US Northern Command, "First Responders – Role of NORTHCOM," n.p., on-line, Internet, 26 February 2004, available from http://www.northcom.mil/index.cfm?fuseaction=s.firstresponders.

[23] Ibid.

[24] Department of Defense, *Joint Vision 2020*, (Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000), 8.

Appendix C

Dominant Characteristics of a Robust P2P Infrastructure[1]

A robust P2P infrastructure has certain characteristics that will be necessary to realize the full potential of the technology and enable a dynamic information-sharing environment.

Dominant Characteristics of Robust P2P Infrastructure

P2P technology offers significant potential to revolutionize how data, information, knowledge and wisdom are gathered, processed and transmitted to, from, and between the edges of the network. However, implementation of P2P technology requires an infrastructure to bring these edges together in a coherent and productive way. Such an infrastructure would provide the standards and protocols that would enable P2P interaction. What would such an infrastructure need to provide to allow the full range of P2P functionality? Endeavors Technology released a first-order attempt to outline conceptually those necessary characteristics. Their white paper explored eight dominant characteristics of a P2P Infrastructure.[2] While these characteristics are not necessarily unique to a P2P infrastructure, P2P technology enables many of these characteristics to be deployed in unique ways that may lend flexibility and robustness.

Placement

The first dominant characteristic that a P2P infrastructure must provide is the ability for peers to place information. The idea of placement includes the ability to add information, search for information, and transfer information without altering its "type." It must remove obstacles that impede the free and seamless transfer of content and services from one peer to another. This would allow content to naturally migrate to where it is most needed and accessed. Given the transient nature of many peers, information destined for them must be held somewhere until they reconnect to the network. Thus, the infrastructure must allow for the "transparent introduction of 'intermediaries,' peers whose role is to cache or migrate content and service from the origin to the point of use."[3]

In the first-responder context, the placement characteristic allows virtually every user and sensor to place information into the "infosphere." This infosphere may be a combination of various disparate systems linked together through a P2P technology. Once linked, the concept of intermediaries could serve as "fusers" to aggregate and fuse data from multiple sources to present a comprehensive knowledge-centric view of the incident-space. One of the more radical capabilities that P2P technology brings is the transformation of control. The users or edge-systems control what information is placed rather than a centrally controlled hierarchical entity.

Security

Security is one of the most difficult problems that P2P technology must address. Thus, security must be foundational to any P2P infrastructure. At a minimum, a robust infrastructure should provide authentication (confirming the identity of a user),

authorization (permission to access a network resource), confidentiality (usually through encryption), and data integrity.

In most networks, security is only as good as the weakest link. However, with security classification restrictions, the various first responder communities will require a relatively robust authentication process to confirm the identity of a network user. With authentication confirmed, the next biggest challenge will be to encrypt the information while it is transiting potentially unsecure or even hostile nodes. In this case, a robust P2P architecture should allow the ability to evaluate the different nodes in the network for their "trustworthiness" and have the ability to remove nodes from the network who prove to be untrustworthy. This reputation establishing function is similar to interpersonal relationship building and is discussed in the security section in the appendix below.

Sharing

P2P technology enables the sharing of information at the edges of the network in ways never before contemplated in the client-server world. However, sharing should be at the discretion of the content or service owner. The creator/publisher of a specific piece of information should have the ability to control what users see and use that information whether they are specific individuals, groups, or devices on the network. This characteristic would be modified by the security characteristic in the appendix below. Four distinct forms of sharing should be supported by a P2P infrastructure:

1. Computation and data storage. This should be shared to maximize the aggregate computing power and data storage power of the network nodes.

2. Content. The ability to share content is foundational to any P2P network and gives value to the P2P concept. However, a robust infrastructure will support the sharing

of metadata that may serve as a surrogate for the data itself.[4] For example, rather than share a large graphic file across the network, a description of the file (metadata) may be all that is necessary until a user needs the entire file.

3. Relationships. Relationships serve as the conduits for the exchange of information. Thus, the ability to share the relationships that one user or device has developed with another user or device must be supported by a P2P infrastructure. This might be simply a list of links that could be passed from one user or device to another. One example of relationship sharing would be the ability to share "buddy lists" between users or devices.

4. Activities. Collaboration is one of the most powerful applications that P2P technology brings to life. The ability for teams of people, who are not co-located, to engage in complex cooperative interactions can be easily enabled by a P2P infrastructure. Since P2P technology can uniquely meet the needs of transient users or devices, users must be able to work independently off-line and then be able to reconnect on-line and share information with the rest of a team. The infrastructure should support the on-line and off-line work in progress and provide a seamless way to interweave both.

The concept of sharing is foundational to P2P technology usefulness in the first responder context. The sharing of computation and data storage, given a secure environment, could have tremendous impact in the near term. Without purchasing expensive, state-of-the-art systems every few months to keep up with current technology, local storage-sharing capabilities could equal or even surpass the newer systems.

Content sharing could enable imagery files or intelligence reports to be shared with others on the network. Relationship sharing could allow the links that one peer (law

enforcement officer, fireman, on-scene commander…) has developed to be shared among other peers. Thus, if a police vehicle is destroyed that is serving as a peer to multiple other peers, the network would be able to reconfigure and absorb the relationships that the police officer had developed. This ability to share links minimizes the impact of a node that is either isolated or destroyed.

Activity sharing is potentially one of the most fruitful near-term applications of P2P technology for the first responder environment. Most first responder activities take place within a team environment. P2P activity sharing facilitates rapid, real-time collaboration. With the shared information resident on each user's device, ad-hoc teams can establish and disestablish quickly and securely without the need for a central server.[5] Thus, the sharing characteristic offers significant potential to multiply the effectiveness of first responder operations.

Governance

If content or service can be owned by the creator/publisher, then a P2P infrastructure should provide the creator/publisher with the ability to control who may use what, when they may use it, and in what manner. This concept of governance may range from simple support for distributed authoring to complex and elaborate digital rights management languages.[6]

For tactical level first responders, classified intelligence information is often limited to the stovepipe of its original collection-centric domain. The governance characteristic may allow intelligence providers to control who gets what information and thus enable information sharing among users that have appropriate authentication and authorization.

This would be especially useful in a homeland security context where different partners have access to different information sources.

Access

Access will be one of the most fundamental principles of any robust P2P architecture. Any device, regardless of its source or capability, should have access to the network. This means that a Personal Digital Assistant (PDA) may be a peer to a high-powered server that may be a peer to a pager. The concept of access "demands that peers acknowledge the underlying differences of platform and negotiate with one another at a more abstract level—that of protocol and service. Homogeneity is the rule rather than the exception in peer computing."[7] Although the devices that are peered may have very different capabilities (bandwidth, processing power, memory, persistence of network communication), access captures the concept of embracing the differences and accommodating them in a systematic and uniform fashion. This will require an infrastructure that allows peers of very different capability and language to interact. Finally, access might mean "larger, resource-rich peers routinely accommodate smaller resource-constrained peers by reducing their service expectations, transcoding content, or acting as proxies for service requests that exceed the capabilities of their less capable brethren."[8]

Control

Control gives the ability to control any peer from any other peer, given the appropriate permission and access. For example, a cell phone may be used to adjust a home climate control system or a PDA may be used to test a remote pumping station.

The P2P infrastructure should enable these types of transactions to take place in a way that is transparent to either user/device.

Specialization

Access and control allow both the users and peers to specialize. This capability allows the user to specify what information he/she wants and how he/she wants it presented (personalization). From the peer's perspective, it is the power to offer peer-specific content and services that differ from other peers (specialization). Ideally, a P2P infrastructure would allow a user to personalize his “space” and then take it with him to wherever he accesses the network (cell, PDA, desktop, laptop…). Furthermore, specialization will allow the actual user interface to be a peer. Specialization provides the infrastructure to allow the user to enjoy the power of choice and select the 'interface peer' that provides just the form of interaction that is desired on the device selected by the user.[9]

For example, the incident response environment may require each first responder to use a PDA in the incident space. Each user will have different needs depending upon his position and responsibility. Thus, the ability to personalize a peer to provide the most accurate and comprehensive information tailored to meet the needs of the first responder will be a powerful tool.

Stewardship

Stewardship encourages peers to seek assistance from other peers in the network. For example, a cell phone may forward the most difficult tasks to a larger, more-capable peer. “Stewardship relieves peers of the burden of providing all services to all peers, thereby permitting large classes of peers to specialize and simplify.”[10] Theoretically,

stewardship would recognize bandwidth and processing power limitations of neighbors and thus self-regulate to prevent bottlenecks or over-tasked peers.

Summary

The eight dominant characteristics of a P2P infrastructure—placement, security, sharing, governance, access, control, and stewardship—capture the most valuable and important concepts that should be present in any P2P infrastructure. Moreover, they expand the ability to conceptually understand P2P technology and its potential applications.

Notes

[1] Much of this information presented in this appendix was originally published in Mark D. Bontrager, "Peering Into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Distribution and Operational Tasking," (Maxwell AFB, Ala.: School of Advanced Airpower Studies, 2001), on-line, Internet, available at https://research.maxwell.af.mil/papers/ay2001/saas/bontrager.pdf.

[2] This white paper serves as the basis for all of the dominant characteristics in this section. Gregory A. Bolcer et al., *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure,* White Paper , (Irvine, CA: Endeavors Technology, 6 December 2000) 7-11; Internet, available at http://www.endtech.com/news.html

[3] Cache (cash): a special high-speed storage mechanism. Many ISPs employ cache servers to keep the most frequently requested web pages handy for quick retrieval when requested by a client. On a personal computer, it can be either a reserved section of main memory or an independent high-speed storage device. (Source: Zdwebopedia, Internet, available at http://www.zdwebopedia.com/TERM/c/cache.html); Bolcer, 8.

[4] Metadata: Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses. (Source: Zdwebopedia, Internet, available at http://www.zdwebopedia.com/TERM/m/metadata.html)

[5] One of the leading companies providing P2P collaboration tools is Groove Networks. Groove is currently providing first-generation P2P collaboration tools to the Joint Staff and other government agencies. More information can be found at Groove's web site: at http://www.groove.net.

[6] Bolcer, 9.

[7] Ibid.

[8] Ibid., 10.

[9] Ibid., 11.

Notes

[10] Ibid.

Appendix D

Promises and Perils of P2P Technology

Promises of P2P Technology[1]

P2P technology is a powerful capability that could potentially link countless users and expose virtually infinite amounts of storage space. However, as with any new technology, it could be misused or create vulnerabilities if not implemented properly and with caution. The promises of P2P technology are directly related to its ability to distribute information and provide robust and dynamic links at the edges of a network. This section will explore some of the advantages that P2P brings and will continue to bring in the future.

First, the major advantage of P2P technology lies in its distributed nature. If implemented with adequate security, P2P overcomes one of the most significant disadvantages of the current client-server framework—the central server. By distributing the nodes, and the information resident on them, there is no single point of attack or failure. This is exactly the same strength of the current Internet, however, P2P technology distributes the information even further to the countless PCs and edge devices connected to the Internet.

Second, the ability of a P2P network to handle transient connections creates an ever-changing network topology that has no critical or central mass. To take down a P2P

network would be like trying to destroy a cloud. If a node is targeted and destroyed, the network can continue to operate without a hitch since it is designed to operate with nodes engaging and disengaging all the time. Thus, the only way to destroy such a network would be to target every node.

This concept is similar to ad-hoc mobile wireless cellular network technology that is currently being developed for Special Operations Forces (SOF). These forces require networks that can be rapidly deployed and that do not rely on any pre-existing infrastructure. Furthermore, given the mobile nature of SOF forces, the ability to maintain a constant network topology is impossible. Thus, the network constantly reconfigures and routes information dynamically rather than through any one primary information node.[2]

Third, one of the most powerful promises of P2P technology lies in the area of relationship creation. With P2P, the edges of the network can link directly and exchange information. Today, in the first responder context, tactical units at the edges of the network link through the use of the radio. Without the radio, coordinated operations are impossible. However, radio communication is primarily limited to voice communications. P2P technology would allow the transfer of data and information in addition to voice to any other peer in the network. Moreover, it would provide the ability to relay relationships with other incident response entities. This relationship-relay would enable rapid network reconfiguration and could provide an on-scene commander with a much richer information environment to enable decision superiority.

Fourth, P2P technology is naturally focused and responsive to users. Rather than information pushed to the user from a provider who *thinks* he knows what the user wants,

the user defines the information that they want and need and how they want it presented to them. Furthermore, applications must be simple to use and clearly value-added or users will not take the time to use them.[3] Thus, competition between interface providers will drive user interfaces that present the clearest, most accurate, most tailorable and most timely picture with the simplest interface. This competition will occur in the marketplace with interface providers competing for business. In the first responder environment, if edge-devices like PDAs become commonplace, there will also be competition to provide the most effective and valuable interface.

Fifth, P2P technology provides a means to save significant resources by taking advantage of the latent, unused computing power resident on a network. Much of the current hierarchical information flow originated because of the limited processing capability at the edges of the network. The edges simply served to relay information back to the more powerful nodes that could perform the processing functions. With the processing power that many edge-devices now have, much of the processing could be accomplished at the edges of the network. In many cases this may be closer to the users and eliminate or minimize the need for "reachback." By processing some information at the edges, only the processed information would need to be transmitted back to a central location. This might help minimize the impact of P2P technology on bandwidth utilization.

Sixth, P2P technology provides the ability to scale to meet the demands of users. One of the limitations of the client-server model is the central server (or servers) that holds the information. If many users try request information from that central server simultaneously, the server may become overloaded and unable to respond to any

requests. Or, it will try to service all of the requests at the same time resulting in decreased service and speed for each user. Furthermore, the bandwidth pipe that connects the user to the server may also become overloaded resulting in the same detrimental effects. P2P technology may help overcome this limitation by distributing the information between many nodes (rather than just one node). If a central repository of information were necessary, another alternative provided by P2P technology would allow a central server to replicate itself on other nodes under its immediate control. The ability to scale to meet increased demand could allow the distribution of storage capacity to non-server entities like PCs or laptops.

Overall, the ability of P2P technology offers many promises that will be explored throughout industry. However, first responder applications of P2P technology may mirror the industrial applications or extend beyond the profit/loss model. In other words, specialized P2P applications may be needed for first responder use that would require government investment to meet the needs of users in the field. Field experimentation with various P2P technologies should yield significant insight into the P2P applications most relevant to first responder users. Moreover, throughout history, when a new technology has been made available, the fielded forces often find a new use for that technology that was never anticipated in the laboratory.

Perils of P2P Technology

The biggest challenges facing P2P technology are anarchy (lack of a central, controlling server), bandwidth limitations, and security. Each of these challenges impinges upon the other with both negative and positive effects.

Anarchy

P2P technology fundamentally removes hierarchical control over information. First, with the no-broker model and each node operating independently and potentially going straight to each other node, the benefits of a centralized Broker were removed. This Broker could direct traffic and cut off those nodes that were unproductive or damaging. Without a Broker, anarchy could lead to very inefficient networks. For example, if many nodes request the same information, each request is relayed across the network until sources are found. A Broker could simply point all of the users to the data without the "overhead" required for relaying multiple requests. Second, while giving freedom to each node to participate or not, it may also negatively affect the whole. Like the real world, "peer-to-peer communities depend on the presence of a sufficient base of communal participation and cooperation in order to function successfully."[4] Thus, in a crisis incident, if traditional power sources are removed, a sufficient number of nodes could be removed from the network and the network could disappear or become bogged down with only a few nodes supporting it.

Bandwidth

P2P technology depends on sufficient bandwidth.[5] The availability of relatively high bandwidth (broadband) providers, combined with the increase in processing power and storage capacity, fueled the P2P mania in 2000-2001. As a result, the early P2P applications needed a lot of bandwidth and without it, they often break down ungracefully. There are a number of reasons for this limitation.

First, P2P depends upon a connection between peers and is limited by the quality of that connection. For example, if a dial-up modem is a peer to a high-speed server, and

the limited throughput capabilities of the modem are not identified, then the modem could be expected to perform like a high-speed server and would be quickly overwhelmed. In this scenario, the network is only as fast as its weakest link. This is what happened with the early Gnutella network. Gene Kan, one of the Gnutella developers writes, "Early Gnutella software would obstinately maintain connections to nodes in spite of huge disparities in carrying capacity. The effect was that modem nodes acted as black holes into which packets were sent but from which nothing ever emerged."[6] One fix to this problem is to intelligently build a network topology that has the fastest nodes at the center of the network and the slowest nodes at the edges. This was done with Gnutella by forcing high-speed nodes to disconnect those nodes that are bandwidth disadvantaged. This process created a virtual network control function and an ad-hoc backbone where, over time, the high-speed nodes migrated to the center of the network and carried the bulk of the traffic.

Second, the no-broker models, without the benefit of a central index, depend upon frequent query searches throughout the network. Each peer must repeat the query until the information is found, or the query times out. This repetition process consumes much bandwidth and can lead to traffic overloads that can slow down the network and its ability to meet requests.

Solutions to the bandwidth challenge are forthcoming. P2P technology is relatively immature and proponents of P2P technology propose that with time, many of the current limitations will be overcome by using techniques described below. Here are some ways that P2P applications are working to reduce the bandwidth demands of the technology.

One of the most promising ways to respond to the bandwidth challenge is to build a rich metadata function that lets users evaluate, with confidence, metadata rather than the file itself. For example, rather than passing a large image file over the network to each user, a much smaller metadata file would be passed. Each user could determine, by evaluating the metadata, if the image file would meet their needs. If so, then the image file could be passed. This would decrease traffic significantly. The biggest challenge will be encouraging metadata discipline by those who would expose information to the network.

Another way to respond to the bandwidth challenge is to duplicate the most popular files throughout the network. In this case, a given file could be hosted by 10,000 individual computers, eliminating the need to use precious bandwidth to access the one location that has the file. This is what many ISPs do today. They capture the most frequently used web pages so that they can serve them quickly to their subscribers. Freenet, another P2P application, also does this without the benefit of a central server. Freenet migrates the most-frequently requested information as close as possible to the people who routinely ask for it. Furthermore, its technology has enough information built in that requests can be routed almost directly to the place where the content is likely to be without having to search every connected computer.[7]

Another solution to the limited bandwidth problem on the Gnutella network was the creation of "super peers" that remember results from other similar searches. Called "Reflectors™," these super-peers index file collections of nodes that connect to it and can subsequently serve as a proxy for these nodes and relieve them from much of the burden of traffic processing.[8] Thus, rather than repeat a common query throughout the network,

and use bandwidth unnecessarily, initial responses can be relatively quick and thorough. (See figure below.)

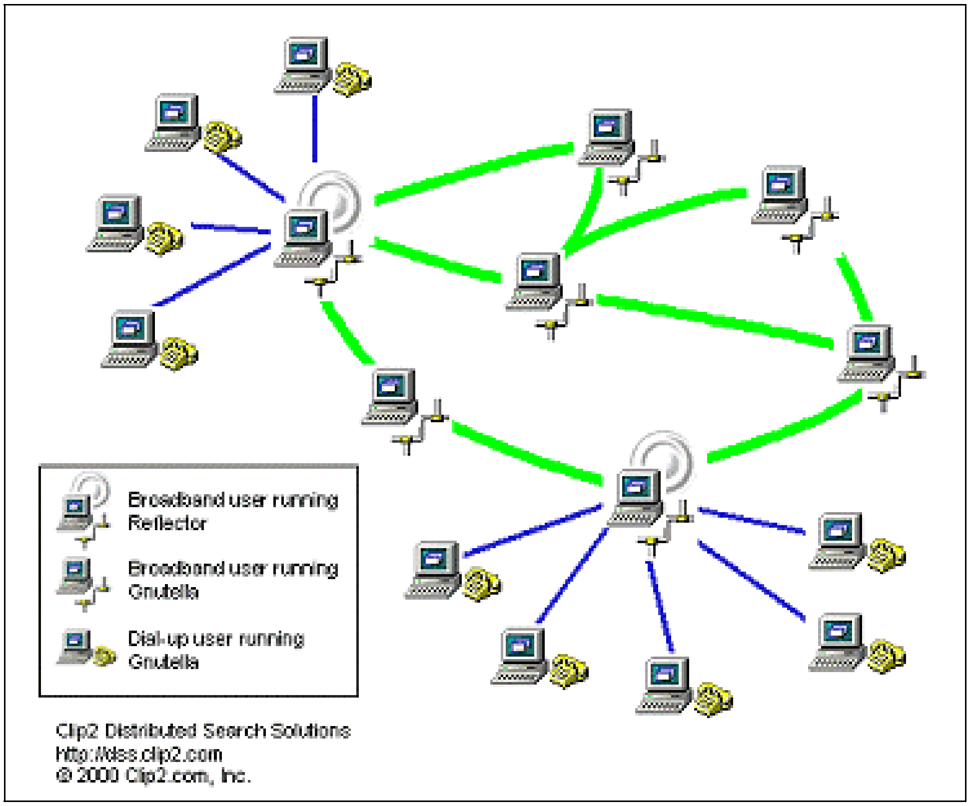

Figure 17. Example Gnutella Network Including Reflectors[9]

Overall, bandwidth demand will be a continuing challenge for P2P technology. However, within the first responder context, nodes on a first responder P2P network may be designed to be good stewards of the limited bandwidth that is available. Moreover, first responders could deploy with applications that already have the maps and key images loaded on the individual systems and thus would require only updates rather than complete information packages. In addition, limited short-range tactical bandwidth, which is currently used for voice, may be able to frequency-share to allow bandwidth for a P2P system. Furthermore, even in the short time since P2P technology became popular,

various quick fixes have minimized the bandwidth limitation problem. It is reasonable to assume that as the technology continues to mature, solutions to the bandwidth limitation problem will be more successful.

Security

Security is one of the biggest challenges facing P2P technology. With the client-server model, servers were the fortresses that held the data and, as a result, were the most valuable targets for attack. Most protection measures focused on protecting the servers from attack from outside the network. One of the most effective tools to prevent unauthorized access are firewalls. Firewalls "stand at the gateway between the internal network and the Internet outside. They filter packets, choosing which traffic to let through and which to deny."[10] They are very effective at protecting a network from attack by denying any entity outside of the network from initiating a connection to an entity inside the network. In other words, "a firewall is like a one-way gate: you can go out [to surf the web…], but you cannot come in."[11] However, they pose a serious obstacle to P2P models because P2P requires the ability to establish two-way sharing relationships with other nodes, regardless of location.

On the web today, secure communications are encrypted between the server and the client using technologies such as Secure Sockets Layer (SSL).[12] Such encryption technologies are used for countless daily web transactions. Moreover, authentication processes are relatively mature to ensure that the server can be trusted.[13] For example, many companies maintain certificates with Verisign[14] who serves as a reliable third-party and "vouches" for the reliability and trustworthiness of its certificate holders. Thus, the

client-server model provides mature security functions to enable confidential transactions.

The challenge for P2P technology is that virtually any device can be a server at some level. Since each peer is untrusted and it is difficult to easily confirm the identity of a transient node with any confidence, security becomes a much more difficult problem than in the client-server model. Moreover, the massive increase in nodes offered by P2P technology may make a network more vulnerable because there are more places to attack. Finally, with the "sharing" characteristic of a P2P infrastructure, viruses and other threats could be quickly and easily shared throughout the network. For example, in November 2000, McAfee Inc. sent out an anti-virus update file that crashed Windows PCs. If that corrupted anti-virus file been sent to a P2P network, the file could have proliferated at an exponential rate.[15]

At a minimum, P2P technologies must address the apparent vulnerabilities of a P2P network. The functions necessary to minimize security breaches are essentially the same as those necessary in any network environment. However, the implementation of security functions has some unique challenges in a P2P environment.

Security Functions

One of the most important functions of any networked system is its ability to authenticate the identity of the users. Authentication merely ensures that the individual is who he or she claims to be. Usually this is done with a username and password. However, with the transient nature of users and machines in P2P systems, a user may use multiple systems and multiple usernames to access a P2P network. Thus, the ability to authenticate becomes extremely difficult.

In response to this challenge, many P2P applications are working to develop a reliable reputation system. For example, eBay, the on-line auction site, allows buyers to comment on the quality of service that they received from sellers. Over time, sellers build either a good or a bad reputation. This works well most of the time, however, if a seller begins to receive a bad reputation, they can just change their username and create a new on-line identity. The reputation and trust building concepts are still in their infancy.

The ability to authenticate may also help determine priority for information traveling through a P2P network. Certainly some information is very time-sensitive and needs to be expedited across the network. For example, the military is distributing "Smart Cards" to all military and contractor personnel. These cards will also contain private keys for digital signatures and access authentication.[16] The same approach could be used to authenticate first responders. With such strong authentication processes in place, P2P technology in the first responder context may offer some significant advantages over the industry context.

Another significant security function is authorization. Authorization determines which resources a user has permission to access based upon their authentication. This relates to the concept of governance that a P2P infrastructure should provide. With governance, the creator/publisher of the information can authorize certain users access to the information. A commercial company called Authentica has developed the ability to govern documents that are distributed by e-mail. For example, with Authentica a user can create a document, attach it to an e-mail, and determine when each recipients can read it and for how long. The recipient can only view the parts of the document that they are given specific permission to view. Furthermore, the ability to view the document can

be revoked at the discretion of the sender.[17] This capability illustrates the power that can be linked with specific authorizations in a P2P network.

Every user of a network needs to know that the information they are receiving has not been altered. This is known as data integrity. Furthermore, in many cases, the information is confidential and must be protected from compromise. Common data integrity functions and encryption routines are used worldwide to provide a fairly high level of security. However, P2P technology may increase the vulnerability of the networked system. In an effort to quantify system vulnerability, the Army Research Labs states, "the likelihood exists that an individual vulnerability of one system in the architecture may in fact snowball and affect other systems that are networked with that particular system."[18] For example, consider the snowball effect of information that is collected and then intercepted and manipulated by a hostile source. The manipulated information could then be spread throughout the network leading to erroneous data that could endanger first responders or even jeopardize mission accomplishment. Thus, data integrity will be another critical function of any P2P infrastructure. The need to provide confidence in the integrity of the data residing on the network will be a paramount consideration.

Security functions will be necessary to provide authentication, authorization, data integrity and encryption. Without robust security functions, P2P technology is vulnerable to the same type of the informational attacks that currently plague the Internet at large.

Conclusion

Peer-to-Peer technology offers dramatic increases in computing power and storage space by empowering and linking the edges of a network. The broker and no-

broker models each offer unique capabilities and limitations. The advantages of a P2P network lie in its distributed nature and its ability to handle transient users and devices. Furthermore, linking the various models may provide more capability than any one model on its own. However, P2P technology may not be appropriate in all circumstances. The client-server model, which has served the Internet very well, is much simpler than P2P, and it would not be wise to abandon the simple for the complex without a clear benefit.[19] Ultimately, a combination of P2P with the client-server model will provide first responders with the flexibility and robust information architecture to enable decision superiority.

Notes

[1] Much of this information presented in this appendix was originally published in Mark D. Bontrager, "Peering Into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Distribution and Operational Tasking," (Maxwell AFB, Ala.: School of Advanced Airpower Studies, 2001), on-line, Internet, available at https://research.maxwell.af.mil/papers/ay2001/saas/bontrager.pdf.

[2] James B. Michael, "Ad Hoc Wireless Communications For Special Operations Forces (SOF)," Naval Post Graduate School, n.p.; on-line, Internet, 8 March 2001, available from http://www.cs.nps.navy.mil/people/faculty/ bmichael/cs4554/SOFNetwork.pdf. Another example of such a mobile communications program is the Situational Awareness System sponsored by the Defense Advanced Research Projects Agency (DARPA). This system uses high-capacity, low-power radios linked together by a self-configuring network to keep soldiers connected with each other. Source: Leopold, George, "Darpa mobile project preps 'soldier's radio,'" EETimes.com, 21 March 2001, n.p.; on-line, Internet, available from http://www.eetimes.com/ story/OEG20010321S0049. See http://www.darpa.mil/ato/programs/suosas.htm for more information.

[3] "CapWIN: Project and Solution Overview," April 2003.???? slide 24.

[4] Theodore Hong, "Performance," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 205.

[5] Bandwidth: The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. The bandwidth is particularly important for I/O devices. For example, a fast disk drive can be hampered by a bus with a low bandwidth. (Source: Zdwebopedia, available at http://www.zdwebopedia.com/TERM/b/bandwidth.html).

Notes

[6] Kan, 108.

[7] John Borland, "Democracy's Traffic Jams," *CNET News.Com,* 26 October 2000, n.p.; on-line, Internet, available from http://news.cnet.com/news/0-1005-201-3248711-2.html?tag=unkn.

[8] Clip2, "Reflector Overview," *Clip2.com*, 4 January 2001, n.p.; on-line, Internet, available from http://dss.clip2.com/reflector.html.

[9] Ibid.

[10] Minar and Hedlund, 13.

[11] Ibid.

[12] Secure Sockets Layer: A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Source: "SSL," *ZDWebopedia*, n.p.; on-line, Internet, 24 February, 2001, available from http://www.zdwebopedia.com/TERM/S/SSL.html.

[13] Nelson Minar, "Security Issues of Peer-to-Peer Systems," Briefing, O'Reilly Peer-To-Peer Conference*,* San Francisco, Calif., 14 February 2001, 5.

[14] For more information, see www.verisign.com.

[15] Dennis Fisher and Scott Berinato, "Making peer-to-peer secure," *Eweek*, 12 November 2000, n.p.; on-line, Internet, 15 March 2001, available from http://www.zdnet.com/eweek/stories/general/0,11011,2652477,00.html.

[16] John Hamre, Deputy Secretary of Defense, memorandum to the Department of Defense, subject: Smart Card Adoption and Implementation, 10 November 1999. As of May 2001, the Army has already started fielding Smart Cards in beta tests that will replace the standard military identification card. Such cards will enable the sending of digital signatures and encrypted e-mail. Source: George Seffers, "Army deploying smart cards," *Federal Computer Week*, 15 May 2001, n.p.; on-line, Internet, available from http://fcw.com/fcw/articles/2001/0514/web-smart-05-15-01.asp.

[17] For more information see http://www.authentica.com. Many companies are now offering similar information control capabilities. Reliable Network Solutions also offers a similar capability. See http://www.rnets.com/product_overview.htm for more information. Another company working with government applications is the Texar Corporations s-Peer network security features. See http://www.p2ptracker.com/news/releases/texar051501.htm for more information.

[18] US Army Research Laboratory, *Digitization and Survivability*, (Aberdeen Proving Grounds, MD: US Army Research Laboratory, 2000), 26.

[19] Andy Oram, ed., *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 396.

BIBLIOGRAPHY

Ahern, Jayson P., Assistant Commissioner, US Customs and Border Protection. Address. E-Gov Conference on Homeland Security, Washington D.C., 2 December 2003.

Alberts, David S., John J. Gartska and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority.* Washington D.C.: DoD C4ISR Cooperative Research Program, 1999.

Anderson, John. Lt Col, Canadian Air Force (CAF), Commander, 426 Squadron, Trenton, Ontario, Interview, 10 February 2004.

Anderson, John W. Former Sheriff, El Paso County, Colorado Springs, Colo., Interview, 13 January 2004.

Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon. n.p. On-line. Internet, July 2002. Available from http://www.co.arlington.va.us/fire/edu/about/after_report.html.

Association of Public Safety Communication Officials (APCO) International. "Homeland Security White Paper." n.p. On-line. Internet, 2002. Available from www.apco911.org.

Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict In The Information Age.* Santa Monica, Calif.: RAND, 1997.

_____. *Swarming and the Future of Conflict*. RAND Report DB-311-OSD. Santa Monica, Calif: RAND, 2000. n.p. On-line. Internet, 22 April 2001. Available from http://www.rand.org/publications/DB/DB311/.

Baird, Zoë and James Barksdale. "Creating a Trusted Network for Homeland Security." Markle Foundation, Task Force on National Security in the Information Age. n.p. On-line. Internet, 26 February 2004. Available from http://www.markletaskforce.org/Report2_Full_Report.pdf.

Bateman, Robert L. *Digital War: A View from the Front Lines.* Novato, Calif: Presidio Press,

Bates, Jason. "U.S. Commander Warns Military." *DefenseNews*, 15 September 2003.

Bergstein, Brian. "Intel to Describe New Chip." *ExciteFor@Home*. 16 May 2001. n.p. On-line. Internet, 17 May 2001. Available from http://home-news.excite.com/printstory/news/ap/010516/19/intel-wireless-chip.

Berkowitz, Bruce D. and Allan E. Goodman. *Best Truth: Intelligence In The Information Age.* New Haven, Conn.: Yale University Press, 2000.

Berners-Lee, Tim and James Hendler And Ora Lassila. "The Semantic Web." *Scientific American.* May 2001. n.p. On-line. Internet, 29 May 2001. Available from http://www.scientificamerican.com/2001/0501issue/0501berners-lee.html.

Bolcer, Gregory A. et al. *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure.* White Paper. Irvine, Calif: Endeavors Technology. n. p. n.p. On-line. Internet, 6 December 2003. Available from http://www.endtech.com/news.html.

Borland, John. "Democracy's Traffic Jams." *CNET News.Com*. n.p. On-line. Internet, 26 October 2000. Available from http://news.cnet.com/news/0-1005-201-3248711-2.html.

Canadian Department of Foreign Affairs and International Trade (DFAIT): Trade and Economic Analysis Division (EET). "Statistics Canada." May 14, 2003. Available at www.dfait-maeci.gc.ca/eet/.

Canadian Forces National Defense Headquarters (NDHQ), Interviews and briefings with various officers a public servants, Ottawa, Ontario, Canada, 11 Dec 03.

Canadian Police Information Centre (CPIC) website. n.p. On-line. Internet, 20 Januar, 2004. Available at://www.cpic-cipc.ca/English/index.cfm.

Canadian Privy Council Office (PCO). Interviews with various members, Ottawa, Ontario, Canada, 11 December 2003.

Capital Wireless Integrated Network Demonstration Project (CAPWIN). "A Study of Best Practices in Information Integration Projects," 7 July 2000. n.p. On-line. Internet, 27 February 2004. Available from http://www.capwin.org/extras/reports/Best_Practices.pdf.

CapWIN Master Presentation. June 27, 2003. Available from the CapWIN Project, 6305 Ivy Lane, Suite 300, Greenbelt, Md. 20770, phone, (301) 614-3700.

Client/Server Architecture. *zdwebopedia*, On-line. Internet, 8 February 2001. Available from http://www.zdwebopedia/TERM/c/client_server_architecture.html.

Clip2, "Reflector Overview." *Clip2.com*. n.p. On-line. Internet, 4 January 2001. Available from http://dss.clip2.com/reflector.html.

CNET. *CNET Glossary*, n.p. On-line. Internet, 24 February 2001. Available from http://www.cnet.com/Resources/Info/Glossary/.

The Combined Communications and Electronics Board. "An Introduction to the CCEB." n.p, On-line Internet. 20 January 2004. Available at the CCEB website found at http://www.dtic.mil/jcs/j6/cceb.

Federal Emergency Management Agency. *Federal Response Plan – Interim*. n.p. On-line. Internet, January 2003. Available from http://www.fema.gov/pdf/rrr/frp/ frp2003.pdf.

Fisher, Dennis and Scott Berinato. "Making peer-to-peer secure." *Eweek*. 12 November 2000. n.p. On-line. Internet, 15 March 2001. Available from http://www.zdnet.com/eweek/stories/ general/0.11011.2652477.00.html.

Foster, Merle. Inspector, and Sergeant Roy Kendall (Technical support) of the Belleville Police Service. Interview, Ontario, Canada, 28 Jan, 04.

Free Peers Inc. "What Is Gnutella." 2001. n.p. On-line. Internet, 25 May 2001. Available from http://www.bearshare.com/gnutella.htm#whatis.

Garcia-Alcoce, Perla. Special Agent, Mexican Instituto Nacional Para el Combate a las Drogas. Interview, FBI National Academy, 186th Session, Quantico, Va., 1996.

Gateway.com. *Gateway_com Glossary*, n.p. On-line. Internet, 24 February 2001. Available from http://www.gateway.com/help/glossary.

Graves, Donald E., Editor. *Fighting For Canada: Seven Battles, 1758-1945.* Robin Brass Studio. Toronto, Ontario, Canada. 2001.

Hamre, John. Deputy Secretary of Defense. Memorandum. To Department of Defense. Subject: Smart Card Adoption and Implementation, 10 November 1999.

Harrington, Caitlin. "Government Reorganization." CQ Homeland Security - Feb. 27, 2004. n.p. On-line. Internet, February 27, 2004. Available from http://www.cq.com.

Hayward, S. et al. *Beyond The Internet: The 'Supranet'.* Gartner Group Research Note COM-11-4753. Stamford, Conn: Gartner Group, 2001, 3. n.p. On-line. Internet, 21 May 2001. Available from http://www3.gartner.com/Init.

Hodgson, Lynn Phillip. Inside Camp X, the Top Secret WW II Secret Agent Training School, Blake Book distribution, Port Perry, Ontario, Canada, 2002.

Homeland Security Act of 2002. Public Law 107-296. 107th Congress. 25 November 2003, Sec 101 (b) (1) (C). n.p. On-line. Internet, 24 February 2004. Available from http://www.cio.gov/documents /pl_107_296_nov_25_2003.pdf.

Howard, Sir Michael. "Military Science in an Age of Peace." *Royal United Services Institute for Defence Studies,* March 1974, 6.

International Association of Chiefs of Police & The Center for Transportation Studies, School of Engineering and Applied Science, The University of Virginia. "The Capital Wireless Integration Network (CapWIN) Project: An Assessment of Select Metropolitan Washington Public Safety and Transportation Agencies User Needs." February 2001.

Integrated Justice Project (IJP). Ministries of the Attorney General and Public Safety and Security 4.03–(Follow-up to VFM Section 3.03, 2001 Annual Report). On-line, Internet. 20 January 2004. Available at http://www.auditor.on.ca/english/reports/en03/403en03.pdf

Internet Engineering Task Force. "The Internet Engineering Task Force." n.p. On-line. Internet, 31 March 2001. Available from http://www.ietf.org/index.html and http://www.ietf.org/rfc/rfc2026.txt.

Internet Corporation for Assigned Names and Numbers. "ICANN Fact Sheet." n.p. On-line. Internet, 25 May 2001. Available from http://www.icann.org/general/fact-sheet.htm.

Jaehne, Dick. USMC Colonel (ret.), Director of the Illinois Fire Services Institute. Interview, 26 Sep. 2003, Champaign, Ill.

Karig, Walter. Commander USNR. *Battle Report: The Atlantic War*. Farrar & Rinehardt, Inc. New York, 1946.

Kelly, Kevin. *New Rules for the New Economy: 10 Radical Strategies for a Connected World.* New York, N.Y.: Penguin Books, 1998.

Knighten, Bob. "Peer to Peer Computing." Briefing. 24 August 2000. n.p. On-line. Internet, 11 October 2000. Available from http://www.peer-to-peerwg.org/downloads/collateral/ 200008_IDF/PtP_IDF.pdf.

Leopold, George. "Darpa mobile project preps 'soldier's radio.'" *EETimes.com*. n.p. On-line. Internet, 21 March 2001. Available from http://www.eetimes.com/story/ OEG20010321S0049.

Liener, Barry M. et al., "A Brief History of The Internet, Version 3.31" Internet Society. 4 Aug 2000. n.p. On-line. Internet, 25 May 2001. Available from http://www.isoc.org/internet/

Lipowicz, Alice. "Ridge Proposes Plan to Link First Responder Radios." *Congressional Quarterly* Homeland Security – Local Response. n.p. On-line. Internet, 23 February 2004. Available from http://www.cq.com.

Lipowicz, Alice and Tim Starks. "Can We Talk? Not Yet, Says an Angry Jane Harman, Targeting Emergency Radio Systems." *Congressional Quarterly, Homeland Security/Technology.* n.p. On-line. Internet, 6 November 2003. Available from http://www.cq.com.

McKinsey Report. "Increasing FDNY's Preparedness." n.p. On-line. Internet, August 2002. Available from http://www.nyc.gov/html/fdny/html/mck_report/toc.html.

Michael, James B. "Ad Hoc Wireless Communications For Special Operations Forces (SOF)." Naval Post Graduate School. n.p. On-line. Internet, 8 March 2001. Available from http://www.cs.nps.navy.mil/people/faculty/bmichael/cs4554/SOFNetwork.pdf.

Michael, Dennis. “Win or lose, Napster has changed Internet.” *CNN.com*, 2 October 2000. n.p. On-line. Internet, 3 October 2000. Available from http://www.cnn.com/2000/SHOWBIZ/ Music/10/02/napster/index.html.
Minar, Nelson. “Security Issues of Peer-to-Peer Systems.” Briefing. O'Reilly Peer-To-Peer Conference, San Francisco, Calif. 14 February 2001.
Money, Arthur L. *Report on Network Centric Warfare: Sense of the Report*. Washington D.C.: ASD/C3I, 2001.
Multinational Interoperability Council (MIC). “Charter.” 2nd Edition, April 17, 2002. n.p. On-line. Internet, 6 January 2004. Available at http://www.defenselink.mil/nii/org/c3is/ ccbm/ mic.html.
Murray, Williamson and Allan R. Millet, eds. *Military Innovation in the Interwar Period.* New York, New York: Cambridge University Press, 1996.
National Defense Authorization Act for Fiscal Year 2003. Public Law 107-314. 107th Congress. 2 December 2002, Sec 901 (a) (3). n.p. On-line. Internet, 24 February 2004. Available from http://www.defenselink.mil/dodgc/lrs/docs/ PL107-314.pdf.
National Research Council. *Realizing The Potential of C4I: Fundamental Challenges.* Washington D.C.: National Academy Press, 1999.
Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). *Information Superiority, Making the Joint Vision Happen*. Washington D.C.: ASD/C3I, 2.
Onley, Dawn S. “First Responders Could get Access to Military Technologies.” Government *Computer News*. n.p. On-line. Internet, 17 September, 2003, Available from http://www.gcn.com.
Oram, Andy, ed. *Peer-To-Peer: Harnessing the Benefits of a Disruptive Technology.* Sebastopol, Calif.: O'Reilly & Associates, 2001.
Peer-To-Peer Working Group. *Peer-To-Peer Computing*. Adobe Acrobat Document, 10. n.p. On-line. Internet, 8 February 2001. Available from http://www.peer-to-peerwg.org/specs_docs/ collateral/P2P_IDF_Rev1.11-web.pdf.
Polisar, Joseph. “Global Leadership in Policing.” *The Police Chief*, v. LXX, number 11, November 2003.
Public Broadcasting Service, “Life on the Internet Net Timeline.” *PBS.org*. n.p. On-line. Internet, 24 February 2001. Available from http://www.pbs.org/internet/timeline/ index.html.
Richard, William S. Brig. Gen. (ret.) 36-year career Signals officer and former J-6 (Signals) for the Canadian Forces. Interview at Queen’s University, Center for International Relations, Kingston, Ontario, 20 Jan 04.
Roman, Lt Col Gregory A. “The Command or Control Dilemma: When Technology and Organizational Orientation Collide.” Research Report AU/AWC/RWP198/96-04 Maxwell AFB. Ala.: Air War College, 1996.
Rosen, Steven P. *Winning the Next War: Innovation and The Modern Military*. Ithaca, N.Y.: Cornell University Press, 1991.
Roy, Peter and Joe Ross. Office of the Chief of Technology, Washington D.C. Metropolitan Police Department. Interview. Washington D.C. 4 December 2003.
SETI@home: Massively Distributed Computing for SETI. *Computing in Science and Engineering*. n.p. On-line. Internet, 8 February 2001. Available from http://www.computer.org/cise/articles/seti.htm.

Shirky, Clay. “What is P2P … And What Isn't.” *O'Reilly Network*. n.p. On-line. Internet, 24 February 2001. Available from http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html.

Sweeney, J. et al. *The Five Peer-to-Peer Models: Toward the New Web*. Gartner Group Research Note COM-12-4447. Stamford, Conn: Gartner Group, 2001, 3. n.p. On-line. Internet, 21 May 2001. Available from http://www3.gartner.com/Init.

Torobin, Jeremy. “Canada Might Give Airline Passenger Flight Data to the U.S.” CQ Homeland Security News. n.p. On-line. Internet, Jan 30 2004, Available from http://homeland.cq.com/hs/.

Turner, Jon. Major, British Royal Army exchange officer commanding the Canadian Electronics and Communications Training Squadron. Interview at the Canadian Forces Base, Kingston, Ontario, 22 Jan 04.

Tuttle, Jerry O. “Decision Superiority and Intelligence,” *Defense Intelligence Journal*, September 2000, 67-71.

Upbin, Bruce “Sharing Power.” *Forbes*. 27 November 2000. n.p. On-line. Internet, 3 March 2001. Available from http://www.forbes.com/forbes/2000/1127/6614278a_print.html.

US Air Force Scientific Advisory Board. *Report on Building the Joint Battlespace Infosphere, Volume 1: Summary.* SAB-TR-99-02. 2000. n.p. On-line. Internet, 25 May 2001**,** Available from http://www.sab.hq.af.mil/Archives/1999/JBI/JBIExecutiveSummary.pdf.

US Army Research Laboratory. *Digitization and Survivability.* Aberdeen Proving Grounds, Maryland: US Army Research Laboratory, 2000.

US Department of Defense. *Joint Vision 2020.* Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000.

US Department of Defense. “Our Bottom Line.” n.p. On-line. Internet, 26 February 2004. Available from http://www.defenselink.mil/pubs/dod101/dod101for2002/dod101for2002_files/frame.htm.

US Department of Defense. “Unified Command Plan.” n.p. On-line. Internet, 26 February 2004. Available from http://www.defenselink.mil/specials/unifiedcommand/.

US Department of Defense. “Unified Commanders.” n.p. On-line. Internet, 26 February 2004. Available from http://www.defenselink.mil/pubs/dod101/dod101for2002/dod101for2002_files/frame.htm.

US Department of Homeland Security. “Department of Homeland Security Organizational Chart.” n.p. On-line. Internet, 24 February 2004. Available from http://www.dhs.gov/dhspublic/interweb/assetlibrary/DHS_Org_Chart.ppt.

US Department of Homeland Security. *US Department of Homeland Security: Preserving Our Freedoms, Protecting Our Nation.* n.p. On-line. Internet, 24 February 2004. Available from http://www.dhs.gov/dhspublic/display?theme=10&content=3206.

US Department of Homeland Security. “DHS has Five Major Divisions, or ‘Directorates’.” n.p. On-line. Internet, 24 February 2004. Available from http://www.dhs.gov/dhspublic/display?theme=9&content=2973.

US Department of Justice. “Federal Bureau of Investigation.” n.p. On-line. Internet, 27 February 2004. Available from http://www.usdoj.gov/jmd/mps/manual/fbi.htm.

US Department of Justice. “Organization, Mission and Functions Manual, August 2002. n.p. On-line. Internet, 27 February 2004. Available from http://www.usdoj.gov/jmd/mps/manual/overview.htm.

US Department of Justice. "Overview." n.p. On-line. Internet, 27 February 2004. Available from http://www.usdoj.gov/jmd/mps/manual/overview.htm.

US General Accounting Office (GAO). Testimony Before the Committee on Government Reform, House of Representatives. "Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues," Statement of Robert F. Dacey, Director, Information Security Issues and Randolph C. Hite, Director Information Technology Architecture and Systems Issues, GAO-03-715T, 8 May 2003, pp. 1-2.

US Joint Forces Command Concepts Division. "A White Paper for The Common Relevant Operating Picture." Draft White Paper, version 1.1., Norfolk, Va.: 21 April 2000.

US Northern Command. "ASOCC Fact Sheet." USNORTHCOM/J6. USNORTHCOM/J6. Peterson AFB, Colo, 2003.

US Northern Command. "First Responders – Role of NORTHCOM." n.p. On-line. Internet, 26 February 2004. Available from http://www.northcom.mil/index.cfm?fuseaction=s.firstresponders.

US Northern Command. "Joint Protection Enterprise Network (JPEN)." "Briefing. USNORTHCOM/J6. Peterson AFB, Colo, 2003.

US Northern Command. "Who We Are – Mission." n.p. On-line. Internet, 26 February 2004. Available from http://www.northcom.mil/index.cfm?fuseaction=s. who_mission.

US Senate. *Authorizing Appropriations For Fiscal Year 2001 For The Intelligence Activities Of The United States Government And The Central Intelligence Agency Retirement And Disability System And For Other Purposes.* 106th Cong., 2nd sess., 2000, S.R. 106-279.

Verga, Peter F., "Homeland Defense." Address. Government Convention of Emerging Technologies, Las Vegas, Nev., 8 January 2004.

ZdNet. Zdwebopedia, n.p. On-line. Internet, 8 February 2001. Available from http://www.zdwebopedia.